potential lawsuits

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Postage PAID at
East Setauket, N.Y.
11733
ISSN 0749 3851

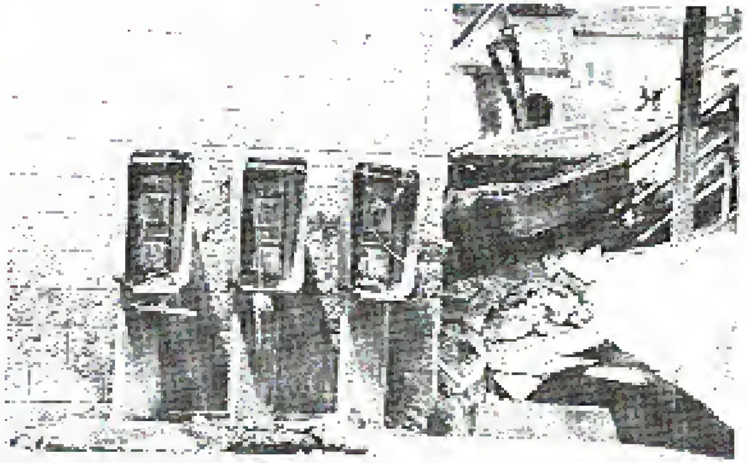
2600

Secret Service
CONFIDENTIAL

The Hacker Quarterly

VOLUME NINE, NUMBER TWO
SUMMER 1992

SAD PAYPHONES



They may not be foreign payphones but they look rather alien to us. These phones happened to be in the wrong place at the wrong time - namely, Los Angeles in the spring of 92. Riots have never been kind to payphones. We can only imagine what the COCOTs looked like.

Photos by Kuang, another 2600 contributor risking his life for the glory of Page 2.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. AUSTRALIA AND SOUTH AMERICA NEEDED!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991
at $25 per year, $30 per year overseas. Individual issues available
from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us

2600 Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

"The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992

Writers: Billsf, Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the identity impaired.

Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

Shout Outs: Steve and friends at CJS, the Northwest Plaza Posse, 5182989953, Franklin, Mike, Fran, Iowa's Mt. Vernon, Mnemonic.

On The Road Again

Portable Hacking

by The Masked Avocado

As the smoke clears from the battlefield, it appears that the enemy has gained a major victory. Scores of people raided, many arrested, some in jail, bulletin boards seized; the casualties are many. Today it is almost impossible to find any hack/phreak board, let alone a decent one. Everyone is laying low, information is scarce. When asked, almost everyone is "retired". Our world is on hold, and has been on hold for what seems like an eternity. The *Phrack* trials, Operation Sun Devil, and a dozen other events have struck a major blow against our way of life, and caused paralysis. Just like in the real world, the phreak/hack world is experiencing a recession of its own.

Raids, of course, have happend many times before, to a lesser extent, and the phreak/hack world has always bounced back. I am sure that the phreak/hack world will come back stronger than ever one of these days. But if it is to survive and avoid another series of raids, then it must change. No longer will we have the comfort of hacking, phreaking, or scanning from home. Those days are over; the enemy has finally learned to use technology too. CLID, ANI, DNRs, narcs, and wiretaps have changed the way of hacking. If we are to survive, then we must change as well. Hacking on the road is no longer an option. It has become a necessity.

History

From the beginning, phone phreaks realized that the surest way to avoid being busted was to use payphones. They called them "phortress phones". Phreaking from a payphone was not that much harder that doing it from home. However, many found this to be an inconvenient, if not a somewhat overly paranoid, option. Given the technology, ignorance, and lack of law enforcement on the part of the enemy at the time, very few were busted. I remember when people set up their computers to hack 950 codes all night, scan entire 1-800 exchanges, and blast all sorts of illegal tones down their home telephone line without giving it a second thought. Today, this kind of behavior is equivalent to suicide. It has gotten to the point where, if you have a DNR on your line, and you actually have the balls to call your favorite bulletin board or (gasp!) call a Telenet port, you could be raided or have yourself hauled in for questioning. Because of easier tracing, recent examples have shown that you can be raided for calling a board, especially one under investigation, perhaps not even knowing that the board was set up illegally on a hacked Unix. Big Brother may be eight years late, but he has arrived. Let us take Darwin's advice, and adapt before we become extinct.

Who Should Go Portable?

Everyone, actually. However, novices and explorers should learn as much as they can from others, and try not to do anything overtly dangerous from home. There is much exploration that is completely legal, like public access Unix machines and the Internet. Those who should go portable right away are experienced hackers, those with a relatively high profile in the hacking community, or those who have many associates in the hacking community. Because of this, they are likely to have a DNR already slapped on their line. Sometimes, all it takes is to have one DNR'ed hacker call another, and the second one has a pretty good chance of getting a DNR of his very own. Enough gloom, let's see what lies ahead.

What You'll Need

Okay, you don't particularly want to get busted by hacking from home, and you want to take your recreation on the road, eh? Well, let us explore the options. Knowing your options and getting the right equipment can make your experience of hacking on the road a less

difficult, more comfortable, and more pleasant one. Depending on the hacker, several factors come into play when purchasing equipment, among them price, power, and portability.

Obviously, one does not need a 486-50DX laptop with an active matrix TFT color screen, 64 megs of RAM, 660 meg hard disk, running Unix V.4 to go hacking. Besides the $13,000 cost, I don't think getting a hernia is anyone's idea of a fun evening. Besides, with a system like that, chances are the laptop you are calling from has twenty times more power than the piece of shit 3B2 with a 40mb hard disk that you're likely to hack into. Similarly, a dinky little pocket computer with a 20x2 flickering LCD screen and a conveniently alphabetized ultra-bouncy membrane chicklet keyboard is not what is needed either.

Important factors in purchasing a laptop or notebook computer are price, weight, screen readability, keyboard, memory, disk storage, and battery life. The price that you can afford should be determined by you. As far as the screen goes, it should be large enough, preferably 80x24 characters, and easy to read. LCD is okay, supertwist LCD even better, EL and PLASMA are even better than that, but if you plan to hack at night or in the dark like most hackers on the road, you should make sure your laptop has a backlit screen. Color LCD screens are useless unless you plan to call Prodigy or download and view GIFs, in which case you should stop reading this article right now and go back to play with your Nintendo.

The keyboard should be a standard full-sized QWERTY keyboard, with full travel plastic keys. You don't need a numeric keypad or function keys or any of that crap. Membrane keyboards or chicklet rubber keys are out of the question. Unless you are utterly retarded, having your keys alphabetized is not an added benefit. Basically, if can touch type on a keyboard without your fingers missing keys, getting jammed or slipping around, then it is a good keyboard.

You don't need a lot of memory on your portable either, since you will mostly be using it as a dumb terminal. However you should have enough memory to run your terminal software and be able to buffer most of your online sessions for later analysis. A floppy drive or some kind of permanent storage is also a good idea. If your portable has battery backed RAM, you may get away without using a floppy drive, since you can always transfer any buffers to a larger machine via the serial port.

The last, and perhaps most important factor in determining your choice for a laptop or notebook is battery life, or more precisely, how long you can use the machine (when it's turned on) before needing a recharge or battery change. Unless you plan to find an AC outlet at every location you hack from, battery capacity is a crucial factor. These battery times vary greatly, anywhere from two hours to 20 hours on some notebooks and palmtops. I would recommend a machine with at least four hours of battery life per charge. If you have a floppy disk drive, your battery life will decrease significantly with each disk access, so try to keep any disk access to a minimum. If your terminal software accesses the disk a lot, I would suggest running it from a ram disk. Having a hard disk on a laptop is pretty useless in relation to hacking, unless your sole purpose in life is to climb a telephone pole so that you can leech all the latest nudie GIFs from Event Horizon's 1-900 number.

"No longer will we have the comfort of hacking, phreaking, or scanning from home."

The laptop and notebook market has changed more quickly than any other segment of the computer industry. New models are literally coming out every three months. While the new models offer better screens and lighter weight, they are usually far too expensive, especially for use as mere hacking rigs. But, an interesting byproduct of all this change is the fact that the older models are constantly being liquidated at almost rock bottom prices by companies like DAK, Demark, and Underware Electronics, which sell by catalog through mail order or by any number of companies that advertise in *Computer Shopper*. The prices are dropping constantly, and by the time you read this article I'm sure the prices I mention will sound high once you've looked through some of these catalogs. Not long ago a friend of mine purchased a brand new 4.4 pound discontinued NEC Ultralight computer with a backlit LCD screen, with a 2MB battery backed silicon disk, and a built-in 2400 modem for just under $500. I've seen a Toshiba 1000 going for $399, Zenith Minisport machines going for $293. If you want, you can pick up a 386SX-20 notebook for under a thousand bucks easily. The point is that the hardware is there, and it's usually far less expensive than any desktop machines.

Modems And Couplers

One does not need a 57,600 baud V.32bis/V.42bis modem to go hacking. Unless you plan to download all of the Unix System V source code from an AT&T mini in under 5 minutes, a high speed modem is not required. A 300 baud modem may be too slow for most purposes, and the only times I would recommend 300 baud is if your notebook or palmtop has a small screen where everything would scroll off too quickly or if you're a slow reader.

A 1200 or 2400 baud modem will do fine. If it has error-correction (i.e., MNP), even better. If your laptop doesn't already have one built-in, I would suggest buying a pocket modem. Pocket 1200 baud modems can be found for as low as $29. Most pocket modems are the size of a cigarette pack and run for 15 hours or so off of a 9 volt battery. Other pocket modems, like the Practical Peripherals' Practical Pocket Modem (Model PM2400PPM, price $159 retail, can be found for $79 mail order) or the Novation Parrot, use low-power chips and run off either the power from your RS-232 port or the phone line voltage or both. These modems are not much more expensive than the battery powered ones, and you never have to worry about your modem running out of power. All pocket modems are Hayes AT compatible and some, like the WorldPort 2496 Pocket Fax/Modem, even have G3 fax capability.

If you're going to be hacking from payphones, you're going to need an acoustic coupler to attach to your modem. Several are available from stores specializing in laptops and laptop accessories. The most popular among hackers is the CP+, available from The Laptop Shop. There's also the Konnexx coupler, which can work with 9600 baud modems and faxes. Look in magazines like *Mobile Computing* for ads for other models. A coupler will run you around $100 mail order.

Ultimately, it is best to keep your portable hacking system as small as possible and made of the minimum number of parts. A notebook machine such as the Tandy WP-2, Cambridge Z88, NEC Ultralight, and the acoustic coupler/modem mentioned above is probably the best possible combination for a compact and inexpensive portable rig. It's small and light, consists of only two or three pieces, fits in a small briefcase or knapsack, and weighs just under five pounds.

By planning and designing your system from start to finish you can achieve a sleek efficient portable hacking system. Poor planning can result in uncomfortable heavy multi-piece systems that one has to drag around. Before laptops really existed, a friend of mine decided to put together a portable rig from parts he already had, and this did not turn out too well. His system consisted of an Apple IIe, a 12 volt car battery, AC power inverter, 9" monochrome monitor, and a full size external Hayes modem. The only things he ended up buying were the inverter and acoustic coupler. However this system was a nightmare of a machine, weighing almost 45 pounds, consisting of seven cumbersome pieces, with tangled cables, and capable of completely draining a fully charged car battery in a matter of 20 minutes. He managed to fit the entire system in a large suitcase. It took him almost 15 minutes to set the entire thing up inside a phone booth, leaving very little room for him. If trouble would arise, he would have a very difficult time making a quick getaway. This is an example of what not to do when putting together your portable rig.

Where To Go Hacking

Location is just as important as having a good portable rig. Where you hack from determines how long you can hack, how late you can hack, whether you'll be bothered by interruptions or have to look over your shoulder every minute, and many other factors. Unless you happen to be travelling around the country and staying in hotels every other week, your only options for portable hacking are payphones, junction boxes, and exposed phone wiring. Finding a great hacking location takes some work, but is well worth the effort. You can save time by surveying locations beforehand, that is, before you actually go hacking. You should find several possible locations that meet your needs. After using one location for a week or so, you should move on. Depending on the sensitivity of the machines you hack, using the same location for an extended amount of time is hazardous to your freedom.

> "Ultimately, it is best to keep your portable hacking system as small as possible and made of the minimum number of parts."

Time of day is also another important factor. It is best to go out late at night to do the majority of your hacking. Besides, 3 am is about the only decent time you can cut into people's phone lines to attach your portable without being noticed. However, 3 am is also when the local cops like to make their rounds through quiet neighborhoods, so be careful, because it's very hard to explain what you were doing inside a junction box to the police, even if you were wearing a lineman's helmet, because linemen don't work at 3 am.

If you don't have an acoustic coupler, you can't really use payphones unless you manage to get access to the wiring. Therefore, you are limited to using whatever telephone lines you can get your wire cutters on. Junction boxes are great, but the ones directly on the street are too dangerous. For all junction boxes, bring along the necessary hex wrench. Almost all junction boxes in suburbia are unlocked and usually very secluded. In the city, however, the best junction boxes are in back of large apartment buildings, or in their basements, or in back of stores and in parking lots. As an added bonus, junction boxes not on the street are not locked. When using a junction box, it is very preferable if you cannot be seen from the street. Junction boxes on poles are also good if you can find them in secluded or remote areas. I found one near me that fits my needs well. It is a huge unlocked box, atop a pole, with a very nice and comfortable seat. What is really great though, is that right next to the pole there's a tree. The branches and leaves of the tree completely engulf the top of the pole, thus I am completely invisible to people passing by on the street. I simply climb the tree to get high enough to start climbing the metal ladder spikes on the pole, and climb up to the seat, unpack my rig, and I'm ready to rock. This is the perfect hacking and phreaking location at 3:00 in the morning. Having access to hundreds of different lines also allows one to use such a location for many hacking sessions before moving on. If you're a college student, dorms are great places to find indoor junction boxes. They are usually in stairwells and in the basement.

If you are not able to use a junction box, all you have to do is find a running line in a secluded location. Again, the backs of apartment buildings and the backs of stores are good places to find wiring. Be sure you know what you are doing, because there is a lot of other wiring that can get in the way, such as cable TV, antenna, and electrical wiring. If you fry yourself on a power cable then you deserve it, because you're too stupid to even go hacking.

If you plan a direct connection (running wiring or junction boxes), other parts you will want to bring along on your hacking trips are a lineman's headset, wire cutters and strippers, and an RJ-11 phone jack with alligator clips.

If you have an acoustic coupler, you have the added option of using payphones and phone booths. But stay away from COCOTs, they are too much of a headache, and the sound quality usually sucks. Good places to find secluded payphones late at night are parks, playgrounds, beaches, and boardwalks. If you live in New York City, then this does not apply to you unless you enjoy being harassed and urinated upon by homeless people while trying to gain root. Obviously, outdoor hacking becomes much less of an option when it rains or when the weather turns cold. During the day, good places to find secluded payphones are old public buildings, college buildings, airports, hotels, libraries, and museums. I once found a phone booth in an old secluded hallway at the Museum of Natural History in Manhattan. This phone was rotary and hadn't been used by humans in I don't know how long. The phone books in there were from 1982. The phone booth was recessed in a wall, well lighted, with a door. Needless to say, this was the perfect spot for several hacking sessions during the day.

With payphones, there is the added problem of the phone constantly wanting money. A red box is very cumbersome, and modem transmissions are immediately killed when the phone wants money every few minutes. Unless your hacking consists entirely of machines with 1-800 dialups, codes or calling cards are a must. Using a phone company with good sound quality, such as AT&T or Sprint, will reduce errors and line noise. Given the acoustic nature of the connection, it becomes necessary to manually flash the switch-hook between calls, and perhaps even manually dialing if your modem cannot autodial. This hassle can be avoided by using a dial-out such as a Unix with cu, an Internet dial-out, or PC Pursuit.

Unlike on TV and in the movies, cellular phones are not really an option for portable hacking, unless you have the ability to completely reprogram yours at a moment's notice, by changing both the Electronic Serial Number and the Telephone Number to someone else's. This type of phreaking requires some advanced knowledge. Getting the ESN's and TN's is not a problem since they are broadcast digitally over the air, and you can pluck them right off the air if you build a decoder and hook it up to a scanner with 800mhz capability. This is, however, a topic for another article. Just as an aside, modem transmissions over cellular phones are quite possible with error correcting modems up to 9600 baud. Telebit even makes a very nice cellular modem called the Cellblazer which can pump data through at 16,000 baud.

"Unless you happen to be travelling around the country and staying in hotels every other week, your only options for portable hacking are payphones, junction boxes, and exposed phone wiring."

Taking to the Road

Another crucial element in successful portable hacking is planning. In light of time constraints and battery life, you should plan as much of your work ahead of time as possible. Any preliminary work should be done before the mission (research, social engineering, etc.). I understand that hacking is somewhat of an unorganized, unplanned activity, but you should at least have some sort of agenda laid out. That's not to say that you can't have any fun or enjoy yourself; you could spend all night calling pirate boards in Europe, for all I care. Nothing is worse than sitting atop a telephone pole at four in the morning trying to think of where to call next.

Be prepared, and bring everything you will need: your rig, handset, notebook, flashlight, food and drink, a list of computers to call, and if you live in New York City, bring along a weapon for self-defense.

When using payphones, it is also a good idea to have a good excuse ready in case someone asks you what you're doing. A favorite among hackers on the road is, "I'm a freelance writer and I'm transmitting a story to my editor." During the daytime at a payphone no one is likely to even notice you since so many people have laptops these days. If you're at a junction box or cutting into someone's phone wiring at three in the morning, no excuse is necessary. Just be prepared to shoot to injure, and run like hell.

During your hacking mission, try to have a good idea of where you are, and make a note of any exits that may be needed if you need a quick getaway. And buffer everything for later review.

The Future

The ultimate thrill would be to carry around a notebook machine with a pocket packet radio TNC and a portable HF transceiver. There are places on the packet nets where you can link into TCP/IP gateways and telnet to any place on the Internet. Also rumored to exist on the packet nets are telephone modem dial-outs. With this kind of setup, you could literally be in the middle of the desert outside of Phoenix, and be hacking a machine anywhere the world. When you're done, you can just move on. I'm sure this scares the shit out of law enforcement, and rightly so. But that may be exactly what we're doing five years from now.

Conclusion

I have been on many portable hacking trips, sometimes alone, and sometimes with friends. All I can really say is that it's a lot of fun, just like regular hacking, but without any of the worries associated with hacking from home. Also, portable hacking is more exiting than just sitting at home in front of your computer. If you find good locations, and bring along a couple of buddies and plenty of good American beer, hacking on the road can be the best thing in the world.

hitchhikers guide to the phone system phreaking in the nineties

by Billsf

Introduction

In this article I will try to introduce you to the most complex machine on earth: the phone system. It's a guide to having fun with the technology, and I hope it will help you on your travels through the network. It is by no means a definitive manual: if you really want to get into this, there are lots of additional things you must learn and read.

This article assumes you know a little bit about the history of phreaking. It is meant as an update for the sometimes very outdated documents that can be downloaded from BBS's. In here I'll tell you which of the old tricks might still work today, and what new tricks you may discover as you become a phone phreak.

As you learn to phreak you will (hopefully) find ways to make calls that you could not make in any other way. Calls to test numbers that you cannot reach from the normal network, calls to ships (unaffordable otherwise), and much more. As you tell others about the hidden world you have discovered, you will run into people who have been brainwashed into thinking that all exploration into the inner workings of the phone system is theft or fraud. Convincing these people of your right to explore is probably a waste of time, and does not advance your technical knowledge.

Phreaking is like magic in more than one way. Those people who are really good share their tricks with each other, but usually don't give out these tricks to anyone walking by. This will be somewhat annoying at first, but once you're really good you'll understand that it's very unpleasant if the trick you just discovered is wasted the very next day. I could tell you at least twenty new tricks in this article but I prefer to teach you how to find your own.

Having said this, the best way to get into phreaking is to hook up with other phreaks. Unlike any other sub-culture, phreaks are not bound by any geographical restrictions. You can find other phreaks by looking for hacker/phreak BBS's in your region. Having made contact there you may encounter these same people in teleconferences that are regularly set up. These conferences usually have people from all over the planet. Most phreaks from countries outside the United States speak English, so language is not as much of a barrier as you might think.

If you live in a currently repressed area, such as the United States, you should beware that even the things that you consider "harmless exploring" could get you into lots of trouble (confiscation of computer, fines, probation, jail, loss of job, etc.). Use your own judgement and find your protection.

Getting Started

The human voice contains components as low as 70Hz, and as high as 8000Hz. Most energy however is between 700 and 900Hz. If you cut off the part under 200 and above 3000, all useful information is still there. This is exactly what phone companies do on long distance circuits.

If you think all you have to do is blow 2600Hz and use a set of twelve MF combinations, you have a lot of catching up to do. One of the first multifrequency systems used was R1 with 2600Hz as the line signalling frequency, but for obvious reasons it is rarely used anymore, except for some very small remote communities. In this case its use is restricted, meaning it will not give you access to all the world in most cases.

To begin with, all experimenting starts at home. As you use your phone, take careful note as to what it does on a variety of calls. Do you hear "dialing" in the background of certain calls as they are set up? Do you hear any high pitched beeps while a call is setting up, as it's answered or at hangup of the called party?

Can you make your CO fail to complete a call either by playing with the switchhook or dialing strange numbers? If you are in the United States, did you ever do something that will produce a recording: "We're sorry, your call did not go through..." after about 15 seconds of nothing?

If you can do the last item, you are "in" for sure! Any beeps on answer or hang-up of the called party also means a sure way in. Hearing the actual MF tones produced by the telco may also be your way in. While it would be nice to find this behavior on a toll-free circuit, you may consider using a national toll circuit to get an overseas call or even a local circuit for a bigger discount. Every phone in the world has a way in. All you have to do is find one!

An Overview of Systems

First we must start with numbering plans. The world is divided up into eight separate zones. Zone 1 is the United States, Canada, and some Caribbean nations having NPA 809. Zone 2 is Africa. Greenland (299) and Faroe Islands (298) do not like their Zone 2 assignment, but Zones 3 and 4 (Europe) are all taken up. Since the DDR is now unified with BRD (Germany) the code 37 is up for grabs and will probably be subdivided into ten new country codes to allow the new nations of Europe, including the Baltics, to have their own codes. Greenland and the Faroe Islands should each get a 37X country code. Zone 5 is Latin America, including Mexico (52) and Cuba (53). Zone 6 is the South Pacific and includes Australia (61), New Zealand (64) and Malaysia (60). Zone 7 is now called the CIS (formerly the Soviet Union), but may become a third European code. Zone 8 is Asia and includes Japan (81), Korea (82), Vietnam (84), China (86), and many others. Zone 9 is the sub-continent of India (91) and surrounding regions. A special sub-zone is 87, which is the maritime satellite service (Inmarsat). Country code 99 is reserved as a test code for international and national purposes and may contain many interesting numbers.

In Zone 1, a ten digit number follows with a fixed format, severely limiting the total number of phones. NPA's like 310 and 510 attest to that. The new plan (beginning in 1995) will allow the middle digit to be other than 1 or 0, allowing up to five times more phones. This is predicted to last into the 21st century. After that Zone 1 must move to the fully extensible system used in the rest of the world.

The "rest of the world" uses a system where "0" precedes the area code for numbers dialed within the country code. France and Denmark are notable exceptions, where there are no area codes or just one as in France (1 for Paris and just eight digits for the rest). This system has proven to be a total mess - worse than the Zone 1 plan!

In the usual numbering system, the area code can be of any length, but at this time between one and five digits are used. The phone number can be any length too, the only requirement being that the whole number, including the country code but not the zero before the area code, must not exceed fourteen digits. Second dialtones are used in some systems to tell customers they are connected to the area they are calling and are to proceed with the number. With step-by-step, you would literally connect to the distant city and then actually signal it with your pulses. Today, if second dialtones are used it's only because they were used in the past. They have no meaning today, much like the second dialtones in the custom calling features common in the United States. The advantages of the above "linked" system is that it allows expansion where needed without affecting other numbers. Very small villages may only have a three digit number while big cities may have eight digit numbers. Variations of this basic theme are common. In Germany, a large company in Hamburg may have a basic five digit number for the reception and eight digit numbers for the employee extensions. In another case in this same town, analog lines have seven digits and ISDN lines have eight digits. In many places it common to have different length numbers coming to the same place. As confusing as it sounds, it really is easier to deal with than the fixed number plan!

International Signalling Systems

CCITT number four (C4) is an early system that linked Europe together and connected to other systems for overseas calls. C4 uses two tones: 2040 and 2400. Both are played together for 150mS (P) to get the attention of the distant end, followed by a "long" (XX or YY = 350mS) or a "short" (X or Y = 100mS) of either 2040 (x or X) or 2400 (y or Y) to indicate status of the call buildup. Address data (x=1 or y=0, 35ms) is sent in bursts of four bits as hex digits, allowing 16 different codes. One hundred milliseconds of silence was placed between each digit in automatic working. Each digit therefore took 240mS to send. This silence interval was non-critical and often had no timeout, allowing for manual working. C4 is no longer in wide use, but it was, due to its extreme simplicity a phreak favorite.

CCITT number five (C5) is still the world's number one overseas signalling method; over 80 percent of all overseas trunks use it. The "plicks" and tones on Pink Floyd's "The Wall" are C5, but the producer edited it, revealing an incomplete number with the old code for London. He also botched the cadence of the address signalling very badly, yet it really sounds OK to the ear as perhaps the only example most Americans have of what an overseas call sounds like!

In actual overseas working, one-half second of 2400 and 2600Hz, compound, is sent (clear forward) followed by just the 2400Hz (seize), which readies the trunk for the address

DTMF is on a 4x4 matrix, one tone from a row and one from a column. 1 = 697+1209, etc.

	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

MF signalling, often used to signal between points, uses a 2 of 6 matrix. Each tone has a weighting which adds up to an unique number. The three standard sets of tones use this system.

DIGIT	WEIGHTING
1	0+1
2	0+2
3	1+2
4	0+4
5	1+4
6	2+4
7	0+7
8	1+7
9	2+7
0 (code 10)	4+7
11 (code 11)	0+12
12 (code 12)	1+12
KP1 (code 13)	2+12
KP2 (code 14)	4+12
ST (code 15)	7+12

For C5, either KP is 100mS and each digit lasts 50mS. A 50mS off time is used between each digit. For older R1 systems, the KP is 100mS and each digit is 68mS on and 68mS off. Modern systems are C5 compatible and use the C5 timing. In North America, an additional 50 or 68mS pause is inserted before the last digit.
Example: KP18(pause)2ST...KP03120600148(pause)0ST. This pattern was added about 15 years ago and appears to be unnecessary, except to give an audible indication of false (blue box) signalling. Its use is HIGHLY recommended for phreaks where it is normally used by the telco! R2 is a COMPELLED system where reception of the forward signal produces a backward signal, which at its reception, stops the forward signal. The stopping of the forward signal stops the backward signal, and when the stopping of the backward signal is detected, a new forward signal is generated. This goes back and forth until all the information is transmitted. The backward signal (usually "1", send next digit) tells the sending end what to send next. See the CCITT Red Book or Welch for complete information on both systems.

WEIGHT	MFC	R2 forward	R2 backward
0	700	1380	1140
1	900	1500	1020
2	1100	1620	900
4	1300	1740	780
7	1500	1860	660
12	1700	1980	540

C4 is the old European signalling system. The address signals have 35mS pause between each beep and 100mS pause (minimum) between each digit. Minimum time to send a digit (including pause) is 345mS. This system is in limited use today, if at all.

x:	2040	35mS (binary "1")	
y:	2400	35mS (binary "0")	
X:	2040	100mS	
Y:	2400	100mS	
XX:	2040	350mS	
YY:	2400	350mS	
P:	2040+2400		150mS

Clear Forward:	PXX
Transit Seizure:	PX
Forward Transfer:	PYY
Terminal Seizure:	PY
1:	yyyx
2:	yyxy
3:	yyxx
...	
14:	xxxy
15:	xxxx
16:	yyyy

PLACE	EVENT	FREQ	CADENCE
N. America	dialtone	350+440	continuous
	ring	440+480	2s on 4s off
	busy	480+620	0.5s on 0.5s off
	fast busy	480+620	0.25 on 0.25 off
England	ring	450+500	0.25 on 0.5 off
(Australia, New Zealand, etc.)			0.25 on 2.0 off
Japan	ring	450+500	1.0 on 2.0 off
Holland	dialtone	150+450 (450 at -8dB)	continuous
most of world	all	400 or 440	(see text)
	SIT	950, 1400, 1800	(see text)

Most of the world's phone systems use only one low pitched tone to represent all calling status. The most common tones in use are 400Hz, 440Hz, and 450Hz. In some cases the tones are modulated, usually AM, at 25 or 50Hz at variable depths. In some old switches, the ring modulates the tone, or it is just the harmonics of the ring frequency, which is usually 25Hz, but can be other frequencies, producing the "fart ring". Cadences for the busy are either the fast at 0.25 on and 0.25 off, or the slow at 0.5 on and 0.5 off. Ring signals are usually on one second and off for two, but can vary. In Iraq, the ring is continuous! The SIT (subscriber information tone) is 950 then 1400 and then 1800Hz. The total length is about one second. The lengths of the individual tones are sometimes variable to impart different meanings for automatic detection.

signalling. All address signals are preceded with KP1 (code 13) for terminal traffic, plus a discriminating digit for the class of call and the number. The last digit is ST (code 15) to tell the system signalling is over. For international transit working, KP2 (code 14) is used to tell the system a country code follows, after which the procedure is identical to the terminal procedure.

CCITT six and seven (C6 and C7) are not directly accessible from the customer's line, yet many "inband" systems interface to both of these. C6 is also called Common Channel Interoffice Signalling (CCIS) and as its name implies, a dedicated line carries all the setup information for a group of trunks. Modems (usually 1200 bps) are used at each end of the circuit. CCIS is cheaper, and as an added benefit, killed all the child's play blue boxing that was common in the states in the 60's and early 70's. In the early 80's fiber and other digital transmission became commonplace, and a new signalling standard was required. C7 places all line, address, and result (backward) signalling on a Time Division Multiplexed Circuit (TDM or TDMC) along with everything else like data and voice. All ISDN systems require the use of SS7 to communicate on all levels from local to worldwide.

The ITU/CCITT has developed a signalling system for very wide and general use. Once called "the European system", R2 has become a very widespread international system used on all continents. R2 is the most versatile end-to-end system ever developed. It is a two-way system like C7 and comes in two forms, analog and digital, both fully compatible with each other. R2 has completely replaced C4, with the possible exception of a few very remote areas where it works into R2 using registers. Two groups of fifteen, two of six MF tones are used for each direction, the high frequency group forward and the low group backward. Line signalling can be digital with two channels or out-of-band at 3825Hz, DC, or in cases of limited bandwidth on trunks, can use the C4 line signals, just the 2040 + 2400Hz or 3000Hz or even backward signals sent in a forward direction. The signals can be digitally quantised using the A-law or u-law codec standards, resulting in compatible signals for analog lines. In international working, only a small part of the standard is mandatory with a massive number of options available. For national working, an ample number of MF combinations are "reserved for national use", providing an expandable system with virtually limitless capabilities. R2 is the "system of the nineties" and mastering this, for the first time, allows the phone phreak "to hold the whole world in his hands" in a manner that the person who coined this phrase could have only dreamed of in the early seventies!

With the exception of bilateral agreements between neighboring countries to make each other's national systems compatible, especially in border regions, all international systems in use are: C5, C6, C7, and R2. R2 is limited to a single numbering region by policy and must use one of the three remaining systems for overseas working. There are few technical limitations to prevent R2 from working with satellites, TASI, or other analog/digital undersea cables. The spec is flexible enough to allow overseas working, but is not done at the present time. R2 is likely to displace C5 on the remaining analog trunks in the near future.

National Signalling Systems

CCITT 1, 2, and 3 are early international standards for signalling the distant end. C1 is just a 500Hz line signalling tone, and was used to alert the operator at a distant switchboard that there was traffic and no DC path, due to amplifiers or repeaters on a relatively long circuit. C1 has only one line signalling function (forward transfer) and no address signalling. It is probably used nowhere.

CCITT 2 was the first international standard that used address signalling, allowing automatic completion of calls. Two frequencies, 600Hz and 750Hz, were used for line signalling and by pulsing between the two frequencies, representing make and break, of the loop current at the distant end during signalling, calls were automatically pulse dialable. You may actually find this system in limited use in very remote parts of Australia or South Africa. Fairly high signalling levels are required and may very well make customer signalling impossible, unless you are right there. Travel to both the above countries should be fascinating however for both phone play and cultural experience!

CCITT 3 is an improved pulse system. On-hook is represented by the presence of 2280Hz and offhook by the absence of 2280Hz. This exact system is still used in a surprising number of places. Pulse-dial PBX's often use C3 to signal distant branches of a company over leased lines. Signalling for this system is generally at a much lower level than C2; the tones will propagate over any phone line.

A system from the early 50's is called R1. Many people remember R1 as the blue boxes of the 60's and 70's. R1 is still in wide use in the United States, Canada, and Japan. The use of 2600Hz for line signalling is quite rare in the 90's, but can be found in all of the above countries. Address signalling uses the MFC standard which is a combination of two of six tones between 700Hz and 1700Hz, as in CCITT 5. Almost all R1 used either "out of band" signalling at 3825Hz or 3350Hz or some form of digital or DC line signalling. To use this system from home one must find an indirect method of using the "out of band" signalling. In North America: most signalling from your central office to your long distance carrier is R1, as is most OSPS/TSPS/TOPS operator traffic.

Pulse systems like CCITT 2 and 3 are still used in national systems. In North America, the C3 standard using 2600Hz in place of 2280 for national working was commonplace through the 70's and still has limited end-to-end use today. "End-to-end" use refers to sending just the last few digits (usually five) to complete the call at the distant end. The only use this may have to the phreak would be to make several calls to a single locality on one quarter. It may be possible that a certain code would drop you into an R1, but you just have to experiment! This type of system is referred to as 1VF, meaning "one voice frequency". The other standard frequency, for use outside North America, is 2400Hz. A national system using using two voice frequencies (2VF) may still be used in remote areas of Sweden and Norway. The two frequencies are 2400Hz and 2600Hz. Playing with these two systems in Europe predates the cracking of the R1 and C5 systems in the late 50's and early 60's respectively. The first phone phreak was probably in Sweden!

Common Channel Interoffice Signalling (CCIS) is CCITT 6 developed for national use and employing features that are of interest to national administrations. R1 often plays into a gateway being converted to CCIS and CCIS will play into a gateway that converts to C5, C6, or C7 for international working. The bulk of the ATT net is CCIS in North America, while R1 is

Do It Yourself Demon Dialer Kit
Hack-Tic Technologies
Postbus 22953
1100 DL Amsterdam, The Netherlands
+31 20 6001480 / *14#
Price based on 350 Deutsch marks
Currently equivalent to US $250

Review by The Devil's Advocate

We Got It

It arrived, inconspicuously enough, in a plain brown wrapper, the Hack-Tic postmarking was enough to inform us of its contents. This was the device that everyone was talking about, this was the box to end all boxes, this was the technology that had corporate and government authorities shaking worldwide, this was the ultimate phone phreaker's tool, the Rainbow Warrior, the God Box, the Demon Dialer. Hack-Tic has responded to AT&T's invitation to "reach out and touch someone" by offering a gem for just such a purpose.

The kit included two printed circuit boards (one for the actual Dialer and the other for the keyboard), a bag of miscellaneous electronic parts (no miniatures, micros, or surface-mounts), another bag containing 13 pushbutton switches, a piece of anti-static foam holding two integrated circuits (the MC68HC705C8P/DD heart of the Dialer and the LM356N3 amplifier), and two instruction manuals (one for Construction & Hardware and the other for Operation & Software). The entire kit comes in a VHS cassette tape box.

Our first observation was that the kit did not include a number of parts that would be needed for final assembly. Missing was a chassis to mount the Dialer in, a speaker to connect the Dialer to, a 25 or 9 pin connector for serial interfacing (yes, the Dialer is quite capable of this!), and a battery snap or holder for the batteries. We were extremely disappointed that the kit did not come with these parts, as they are not superfluous but absolutely essential for the often used by your CO to talk to it and the lesser networks. CCITT 7 is the digital system and is the same nationally as internationally. C7 allows the greatest efficiency of all systems and will in time be the world system. C7 has much more speed and versatility than R2, but is a digital only system. All fiber optic systems employ SS7 (C7).

No discussion of systems is complete without mentioning Socotel. Socotel is a general system developed by the French. It is a hodgepodge of many systems, using MFC, pulse tone, pulse AC, and pulse DC system. Most (all?) line signalling tones can be used. An inband system can use 2500Hz as a clear forward and 1700 or 1900Hz for seize or, in Socotel terms, "confirm". Most line signalling today is "out of band", but unlike normal outband signalling, it is below band: DC, 50Hz or 100Hz. It is a "brute force" system using 100V levels, insuring no customer has a chance of getting it directly! Call setup on the AC systems often has a very characteristic sound of short bursts of 50Hz or 100Hz buzz, followed by the characteristic French series of 500Hz beeps to alert the customer that the call has been received from the Socotel by the end office and is now being (pulse) dialed. Calls often don't make it through all the gateways of a Socotel system, sometimes giving the French phreak a surprise access where it stuck!

On a national level there are even more systems and some are very bizarre. Some use backward R2 tones in the forward direction for line signalling, giving analog lines the versatility of digital line signalling. There have been some interlocal trunks that actually used DTMF in place of MF! The "Silicon Valley" was once served by DTMF trunks for instance. When I visited my local toll office and was told this and pressed for an answer as to why, I was told "We had extra (expensive then) DTMF receivers and used them!" As a phreak, be ready for anything as you travel the world.

Stuff to Read

Signalling in Telecommunications Networks, S. Welch, 1979 ISBN 0 906048 04 4. The Institution of Electrical Engineers, London & New York.

CCITT Red Book, Blue Book, Green Book and whatever other colors of books they have. Concentrate on the Q norms.

Telecommunications Engineering, Roger L. Freeman.

operation of the Dialer. In addition, it can take some time to order the requisite parts from electronics firms, and this additional wait can be frustrating to anyone who has assembled the Dialer and wishes to test it. Fortunately, we at 2600 were able to find some spare parts around the office, although the aesthetics of our Dialer suffered from our impatience.

We Built It

Constructing the Dialer was easy. Unlike the earlier versions which used difficult-to-solder surface-mounted devices, the new model practically snapped together, and will offer no serious challenges for anyone who knows how to solder. The Construction & Hardware reference manual was clear and concise, explaining the soldering pitfalls of each part, what to avoid, and how to troubleshoot. We found it comforting to know that, with the exception of the main chip, the parts to the Dialer are easily obtainable in case of any major soldering catastrophe.

Naturally, you will need a soldering iron rated for 30 watts or less, as well as rosin core solder. Expect to take two hours to solder the boards, and another hour to mount the boards, battery, and speaker into the chassis. Mounting can take quite some time as you must cut holes in the chassis to allow the keys to poke through from the inside. A template is provided to make this job easier.

At first glance, the Dialer may not seem to be big, but once you add the speaker and battery, you will find that everything adds up. Although Hack-Tic claims that a fully assembled Dialer will fit inside a king-sized cigarette box, you will find that the device will need at least a 2" by 2" by 1" chassis, and this is assuming that you are using the thinnest speaker and 6 volt battery that money can buy.

We Turned It On

The Dialer has 13 keys: 0 - 9, # (pound), * (star), and ^ (shift). Pressing the shift key powers up the device, which responds with a short upward tone sweep. At this point, the device will act like a regular touch tone dialer in all respects. In order to access any special features, you must first enter a unique password that is included with the kit. Failure to enter the correct password upon immediately powering up the Dialer means that you must wait 30 seconds until the device powers down before you can try again. And just how secure is this password protection? According to the manual:

"The program in [the main chip] (which also contains your password) is protected by a security-bit that tells the processor not to allow the outside world to read the contents of its PROM. We do not know of any methods to read the contents of a security-bit protected PROM short of probing on the surface of the chip itself.... In other words, it is *very hard* for someone who does not know the code to prove that your device is anything but an ordinary DTMF-dialer."

According to Hack-Tic, the passwords are not archived anywhere so you should not forget what it is. In addition, you should be careful when entering the password as the touch tones will sound and can be decoded. Because the password is burnt into the PROM, it cannot be changed, although you can turn the password protection on or off anytime, but only after you have access to the special features. When the password protection is turned off, the Dialer will automatically power up in the mode where it was last left. You will find this useful when you are programming macros, as this can take some time and the device will often power down while you are thumbing through the manuals.

If you don't want to wait 30 seconds for the device to power down, you can immediately power down by pressing "^*^*" (shift, star, shift, star). (Anyone who doesn't know the password cannot do this unless you turn password protection off.) You may also wish to connect your own on/off power switch to keep the unit from accidentally powering up when something brushes against the shift key. Simply wire your own switch in series with either the positive or negative lead of the battery. The only drawback to using your own switch is that the Dialer will lose everything you programed in RAM every time the power is disconnected.

The password protection was included in the software with Americans in mind. If you are "caught" with the Dialer, it will be up to the authorities to prove that what you have is nothing more than a regular touch tone dialer. We were detained in just such a situation when U.S. Customs Inspector Kaufman (badge number 29439) decided to expand his limited technical prowess by inquiring into the device. We explained that the "thing with buttons" was a dialer (no lie there!) and that we used it to access our voice mail system (among other things). After thoroughly playing with the Dialer, Kaufman accepted this explanation with little more than a veneer of suspicion, and should be happy to know that his ignorance in not confiscating the Dialer is what made this review possible. From all of us at *2600*, thank you Inspector Kaufman!

We Played With It

The Dialer has a total of 12 modes, as well as a number of special functions. Switching from one mode to another is easy, and it doesn't take long to learn where everything is.

Each mode number is followed by its attributes.

0: touch tone (DTMF, White Box, Silver Box).

1: ATF1.

2: R2-Forward.

3: CCITT No. 3, pulse dialing for hooking the Dialer directly to a phone line. A schematic for this operation is included, but not the parts.

4: CCITT No. 4.

5: CCITT No. 5/R1 (Blue Box, KP1, KP2, MF, ST).

6: Coin-signalling tones (Red Box for ACTS, IPTS, and non-ACTS).

7: Line-signalling tones.

8: Tone-slot

12: R2-Backward.

18: user programmable (see below).

The Dialer also sports a macro mode that allows any combination of the above modes, nesting, aliasing, pausing, and retry. You could for instance set up a macro to Red Box, wait until a key is pressed,

(continued on page 35)

bellcore's plans for caller id

Bellcore has issued a technical advisory (TA-NWT-000030) that details data transmission standards for future Caller ID services. The services directly referred to are: Calling Number Delivery (CND), Calling Identity Delivery on Call Waiting (CIDCW), and Calling Name Delivery (CNAM). While much of the technical data is already known, there are some significant new bits of information we feel people should be aware of.

Vital Statistics

The signaling interface consists of three layers. The first is the physical layer which defines the requirements of analog data transmission.

The transmitted data signal has to meet these parameters:

Modulation Type: continuous phase binary frequency shift keying.
Mark (Logical 1): 1200 +/- 12 Hz.
Space (Logical 0): 2200 +/- 22 Hz.
Signal Level: -13.5 dBm +/- 1 dB at the point of application to the loop facility into a standard 900 ohm test termination.
Signal Purity: Total power of all extraneous signals in the voiceband is at least 30 dB below the power of the signal fundamental frequency.
Source Impedance: 900 ohms + 2.16 uF nominal.
Transmission Rate: 1200 +/- 12 baud.
Application of Data: Serial, binary, asynchronous.

The second layer is the Data Link Layer that deals with error detection through CRC. The third and final layer is called the Presentation Layer. Here, data is converted into ASCII text in a form readable by the customer equipment (Caller ID devices).

Both single and multiple data messages are supported. Single data message format consists of Channel Seizure Signal; Mark Signal; Message Type Word; Message Length Word; Message Word(s); and Checksum Word. Multiple data message format consists of Channel Seizure Signal, Mark Signal; Message Type Word, Message Length Word; the first Parameter Type Word, the first Parameter Length Word; the first Parameter Word(s); any additional Parameter Type Words, Parameter Length Words, or Parameter Words; and Checksum Word.

Each data word consists of an 8-bit data byte. Each data word is preceded by a start bit (space) and followed by a stop bit (mark). Mark can be transmitted between any two words to maintain a continuous signal and cannot exceed 10 bits. The message length word contains the number of words in the message following it, with the exception of the error detection word.

The channel seizure signal is 300 continuous bits of alternating 0's and 1's. This signal is only used for on hook data transmission and is followed by a mark signal (logical 1) before the actual data is sent. For future off hook data transmission, each data message is preceded only by the mark signal.

The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz). The message type word indicates the service and capability associated with the data message. For instance, the message type word for CND is 04h (00000100).

In an on-hook state, data transmission takes place between the first and second rings. Transmission doesn't begin until 500 ms of silence has elapsed and has to end at least 200 ms before the next ring begins. This allows for between 2.9 and 3.7 seconds for the entire transmission.

An example of a typical on hook CND message follows:

04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51

04 = Calling Number Delivery Information code (message type word)
12 = 18 decimal - number of data words (date, time, and directory number words)
30 39 = 09 ASCII - September
33 30 = 30 ASCII - 30th day
31 32 = 12 ASCII - 12:00 pm
32 34 = 24 ASCII - 24 minutes (12:24 pm)
36 30 39 35 35 35 31 32 31 32 = 6095551212 ASCII - calling party's directory number
51 = checksum word

Future Features

In an off hook state, speech transmission will be interrupted for the duration of the data transmission. A tone will be sent for 80-85 ms to alert the customer (CPE Alerting Signal). This tone will probably be a combination of 2130 Hz and 2750 Hz sent at a nominal level of -16.5 dBm/frequency. Bellcore's explanation for using these particular tones: "The tone to be generated... must be detectable in the presence of near-end speech and provide for minimal occurrence [sic] of false detections.... In addition, the tone must be of tolerable duration and amplitude from a human factors perspective. One of the options that was proposed for such a tone was the DTMF A. This tone did not meet all the performance criteria. As a result, Bellcore researched other options, namely the use of higher frequency dual tones. Based on prior research in Great Britain, Germany, and Japan, it has been established that signal detection performance improves significantly when the alerting signal falls in the upper part of the speech band. For dual tones the frequency pair selected should avoid common harmonic relationships such as 2:1, 3:2, 5:3, etc.... Although studies and testing will continue, we expect that this frequency pair will be the final specified alerting tone for the off hook case.") After sending the alert tone, the central office will initiate a 100-120 ms acknowledgement timer and will wait for an acknowledgement from the customer equipment. An acknowledgement signal will consist of either a single DTMF D signal (for the least sophisticated customer equipment) or a DTMF D signal followed by a delay of 45-50 ms, then another DTMF key (0-D) (to identify more sophisticated customer equipment). Each DTMF tone must have a minimum duration of 40 ms. The actual data will then be transmitted by the central office within 70 ms of the end of the acknowledgement or after the maximum time for an acknowledgement has passed, whichever is greater. If an acknowledgement is not received, the data will not be transmitted and the speech path will be restored.

Right now, one of Bellcore's biggest concerns is the length of the speech path disruption, which can be close to four seconds long. Whether or not customers are willing to put up with that every time another call comes in remains to be seen.

Fun Things To Know

On June 27, 1992 our #5 crossbar switch was retired, ending a long and stubborn mechanical era for us. We're still getting used to our brand new #5 ESS but it's clear that things will never be the same. Our rings sound just like everyone else's, our busy signals no longer have that grating sound, and lots of little tricks no longer work. But now we can finally play around with such standard features as Call Waiting, Call Forwarding, and Three Way. And there are some new tricks, such as the number we discovered that *completely* disables payphones for a *very* long time. And then there's the speed factor: calls are processed incredibly fast. Long distance calls are connected as quickly as local ones used to be. What does our cutover prove to us? Our world is getting smaller; soon the term "long distance" will be a misnomer. And no matter how technology changes, there will always be something to play with.

***

Many people in our area are pretty upset with New York Telephone. Earlier in the year when the Public Service Commission approved Caller ID, there were certain stipulations. New York Telephone had to agree to allow blocking at no charge. In other words, if someone didn't want their phone number to be displayed at the calling end, they could permanently block that feature on their phone. But what nobody knew about was *69 (Call Return). This spring, *69 started to become activated throughout the 516 area code. People found out about it and spread the word. Then New York Telephone announced its existence. What *69 does is allow you to return the last call placed to your number, whether or not you answered the phone. But here's the kicker. There's no way to block this. In other words, it is no longer possible within 516 to call someone directly without them being able to call you right back. This feature was never mentioned at the PSC hearings and many consumer-minded officials are livid with rage. Since this feature works throughout the area code, it is very easy to obtain someone's phone number, even if it's unlisted. All a person has to do is *69 the call, wait for an answer, then look on the local itemization section of their phone bill. But, says the phone company, this is not Caller ID. It doesn't really matter what it's called. Our privacy is going right out the window. [For a detailed look at *69 and how to defeat it, turn to page 31.]

***

According to Wisconsin Bell, even though Caller ID is not yet available to its customers, their numbers may be transmitted to people in other states, if those people subscribe to Caller ID. While this is limited to those states served by Ameritech, this service is going nationwide even quicker than we anticipated. Customers in Wisconsin can dial *67 to block transmission of their numbers at no charge. For now this only applies to customers in the Milwaukee area. Wisconsin Bell claims "the technology is not in place to transmit telephone numbers" in other parts of the state.

***

More Wisconsin news: Simplex hackers there were recently shocked to discover that the combination lock defaults used on Federal Express and UPS dropboxes throughout the entire nation didn't work in Milwaukee. Apparently the managers of those operations are measurably smarter than all of the others in the country who had never bothered to change the original pushbutton settings. As reported in the Autumn 1991 issue, having the same nationwide combination means that every Federal Express and UPS dropbox can be accessed in about one second. So we tip our hats to those who had the foresight to change the settings in Milwaukee. A postscript: by dusting the buttons on the Simplex locks and waiting a day, the hackers were able to open both the Federal Express and the UPS boxes within ten seconds. Sometimes all the planning in the world makes no difference if there's no security to begin with. We should point out that Airborne Express dropboxes are starting to pop up - they use *key* locks, just like real mailboxes. Life continues to move in circles.

***

One of the highlights of the annual Summercon gathering of hackers in St. Louis this June was an incident that took place in a local mall. One of the hackers was ordered by mall security to stop wearing his baseball cap backwards. A sign at the entrance to the mall read "Clothing must be worn in the manner in which it was intended." It seems that security felt this would be a signal for gang members to attack. Rather than deal with the real problem, they believed that it would be better to curtail some freedom of expression. In response to this, other hackers went to Sears and bought more hats, wearing them in unintended manners. Security guards swarmed in and eventually succeeded in driving the intruders out after a lengthy debate. The Northwest Plaza is safe for another year. You may want to call them to ask about their creative use of logic. Their numbers are 314-298-2624 (information), 314-298-0071 (management).

***

Members of *2600* were recently harassed by U.S. Customs agents as they returned to this country from Canada. The agents were extremely suspicious when they saw copies of *2600* and demanded to know what they were writing about. They also took a strong interest in our demon dialer (see page 17), our Simplex hacking tape, and a couple of wireless transmitters (from the schematics published in our Winter 1991-92 issue). After a couple of hours of being searched and interrogated and having all kinds of information about them entered into a computer, our writers were allowed to enter their country once more. The agents admitted they could find nothing illegal. Their biggest suspicion was the wireless transmitters. "We thought you might use them to rip off an ATM," they said. If you haven't already started praying for our future, now would be an excellent time.

***

This number was given to us inadvertently by a long distance operator: 011-44-81-985-3611. This was the direct dial number to London information. Since AT&T has gone from providing free overseas information to charging $3.00 a shot, this direct number was much more economical. But it seems word got out and the number has been changed to something we cannot dial: 011-44-9-10001000. Can anybody figure out how to get through to this? While we're asking questions, does anybody know the justification for charging so much more for information than for the call itself? To us it's twisted logic that will surely result in less calls being made.

***

When Europe finally becomes unified, they will have a common number to dial for emergencies. At the moment, that number is set to be 112. But they may want to reconsider that choice. British Telecom hooked up an exchange in Eversley as a test to respond to both the present 999 emergency number and the future 112. The police have been deluged with false alarms. It seems that whenever telephone lines are being repaired, they make and break electrical contact a few times as they are secured. These random pulses happen to dial 112 a whole lot more than 999. It should be an interesting transition.

***

Sleazy magazine section: *PC Computing* recently printed a dialog between computer security expert Donn Parker and a hacker named Phiber Optik that took place at a conference in 1991. Included within the article was a picture of Parker talking to someone else wearing a nameplate that said Phiber Optik. Since the magazine set up the photos, they obviously knew this wasn't the real person. We want to know why they printed this picture without mentioning that fact. They were unable to come up with an answer for us. They probably figured hackers are *such* outlaws that they'd never bother to stand up for their integrity. Whatever they imagined, it can't compare to the way *Telecom Reseller* portrays hackers. According to this fine piece of journalism that appeared on their front page, "the hackers' business is to sell long distance service to their customers using *your* telephone system to place the call." In another section, "hackers and their customers are greedy. They will not stop until all of the available paths are in use." *Telecom Reseller* calls itself "A Publication for End Users of the Secondary Market." Secondary is certainly an appropriate word for this trash. We find without fail that whenever hackers are portrayed in such an evil light, the person describing them is trying to sell something. No exceptions to that here.

***

AT&T recently announced a new nationwide computerized directory assistance service called "AT&T Find America", billing it as the fastest, easiest way to access the directory assistance databases of Local Exchange Carriers. Using a PC, customers will have dial-up access to AT&T's Accunet packet network, which is linked to most major Bell operating companies' databases. The service will purportedly be "ten times faster" than calling a live operator.

Unfortunately, the dial-up service requires a $500 software package, a $500 monthly subscription fee, and a $100 ID and password registration fee. After that, one only need pay the $22 hourly connect charges plus 40 cents per screen viewed. Assuming three calls per day for a year, that comes to about $6.79 *per lookup*.

Maybe AT&T should take a lesson from the French telephone company, which has been *giving away* free computer terminals and directory assistance services to all of its customers for years. If you want to pursue this latest AT&T venture, call 800-243-0506 and ask for their free IBM demo disk and literature.

***

We recently received this letter from Cable and Wireless: "The Cable and Wireless Network Security Department has been extremely conscientious in recognizing abuse as soon as it occurs. However, computer hackers have infiltrated many customers' travel authorization codes. In order to secure our customer's [sic] travel authorization codes more effectively, Cable and Wireless will block '950' access. It will now be necessary for Cable and Wireless to join the other long distance carriers and issue '800' access. Because the '800' access requires the entry of two extra digits (travel code) this will greatly minimize the chance that a hacker will be able to break your code." Quite frankly, we're surprised. Up until now, Cable and Wireless has been one of the better long distance companies. By continuing to provide 950 service, it was possible to make local and long distance calls from any location (particularly payphones) at rates comparable to directly dialed residential rates. By switching to an 800 number, these rates are no longer economical, even though Cable and Wireless doesn't have a surcharge. At 53 cents a minute, it won't take long for Cable and Wireless rates to far exceed those of other companies that do have a surcharge. What bothers us the most here is the deception involved. Computer hackers are being blamed for something that obviously is not related to them. If it were a simple matter of adding two numbers to an authorization code, why in heaven's name couldn't they just add two numbers and keep the 950 access? Like all other phone companies, Cable and Wireless now believes that making it harder to make phone calls will somehow make them more money. We're sorry to lose the only phone company we ever considered to be a friend. . .

Here We Go Again

The United States Department of Justice along with the Federal Bureau of Investigation and the Secret Service announced another round of hacker indictments at a press conference in New York City on July 8. Five hackers were charged with such crimes as conspiracy, computer tampering, illegal wiretapping, computer fraud, and wire fraud.

The five are most commonly known in hacker circles as Phiber Optik, Acid Phreak, Scorpion, Outlaw, and Corrupt. Each entered pleas of not guilty in federal court on July 16.

And for the first time ever, the government has admitted using wiretaps in a hacker investigation as a method of obtaining evidence.

Repercussions

This case is troublesome for many reasons. Wiretapping alone ought to be enough to send shivers down the spine of the hacker world, indeed the world in general. By justifying such an act, the government is now saying that hackers are in a league with the most notorious of criminals - mobsters, terrorists, and politicians. If this action goes unchallenged, this is the way hackers will be perceived in all future dealings. We feel the government wishes to convey this image simply to make it easier to subjugate those it perceives as a threat.

By tapping into phone lines, the government will claim that vital evidence was obtained. Translation: they will do it again. And what assurance do we have that this method will stop at hackers? None. Wiretapping is certain to become increasingly easy in the future, especially if the FBI is successful in its bid for a mandatory surveillance system on all digital phone systems. (They're already claiming that this case proves how badly they need such a system; we have trouble following their logic.)

With the wiretapping comes the realization that *2600* is also under tightening scrutiny. Since we have been in contact with these hackers for years, since some of them have been at our office, and since they all make appearances at the monthly New York *2600* meetings, we could easily be considered "known associates" of major criminals, possibly even co-conspirators. This means that it wouldn't be very hard for the authorities to justify monitoring our every movement, tapping all of our phone lines, monitoring our data traffic, and doing whatever else they deemed necessary for the likes of us, major criminals that we are. And the same for all of *our associates*.

Despite all of our warnings and protestations over the years, the image of hackers has been portrayed in increasingly ominous tones by the government and the media, despite the lack of substantial evidence that hackers are anything more than overexuberant teenagers and young adults, playing with toys that have never before existed.

If our assessment is correct, then we will not be the last in this chain of suspects. Everyone who has ever expressed interest in the "wrong things" or talked to people in the "wrong crowd" will be subject to surveillance of an increasingly comprehensive nature. And silence is the best way to ensure this.

Fallout

Equally troublesome is the reaction of some members of the hacker community to these recent happenings. There are some that have openly expressed happiness at recent events, simply because they didn't like the hackers involved. A combination of unhealthy rivalry and gross generalization has helped to create an environment perfectly suited to carrying out the government's agenda. Hacker versus hacker.

Over the years, various hacker "groups" have existed in one form or another. PHALSE was formed in the early eighties. Its name meant "Phreakers, Hackers, And Laundromat Service Employees." The FBI regarded them as a closely knit conspiracy. In actuality, few of the members had ever even met each other and spent most of their time trying to figure out how to communicate so they could trade fragments of information. We're told the "laundry connection" was thoroughly investigated by the government even though the words were only included in order to form the PHALSE name. So much for conspiracies. Next was the Legion Of Doom, commonly known as LOD. In 1990, headlines screamed that these techno-anarchists had the potential to disrupt our lives by possessing the E911 "program" which they could no doubt use to manipulate emergency calls everywhere. Sure, it turned out that it wasn't really a program they had but merely a ten page administrative document. And it wasn't really worth $80,000 like Bell South claimed, but a mere $14. It was still enough to send three hackers to prison and plunge the than-publisher of *Phrack* into near-bankruptcy to defend his First Amendment rights. More recently, MOD has been portrayed as the group of potential terrorists that the government needs and the media wants. MOD (nobody really knows what the letters stand for) has developed a reputation of being "evil" hackers. The difference here is that this reputation actually exists *within* the hacker community.

How did this happen? The same naivete that has so firmly gripped prosecutors and hacker haters over the years has made a direct hit upon parts of the hacker community. MOD was no better organized than PHALSE or LOD, either collectively or individually. Nobody knows how many "members" there were. In fact, it's been said that anyone who wanted to be a part of the group merely had to add the letters MOD after their name because nobody could stop them from doing it. Hardly a well organized group, if you ask us. Yet they were perceived as a threat by some, and thus became all the more dangerous.

We certainly don't mean to minimize any damage or harassment that may have occurred. If proven, such actions should be punished, but within reason. So should any acts which involve tangible theft or selling of unauthorized access. This has always been our position. But to blame the actions of a few (possibly even one) on an entire group, real or perceived, is dangerous. This is something history should teach us, if common sense doesn't.

We've taken a lot of heat for our position on this but we must stand firm. Innocent people are being prosecuted for things they did not do. We know this to be true. And we intend to stand up for them. We cannot judge each other on anything less than individual actions.

If we turn against each other, whatever community we have established will unravel completely. It is in the interests of some to have this happen and we don't doubt that they are encouraging acts of disunity. We have to be smart enough to see through this.

A year ago we warned of the dangers of hacker "gangs" and "elite" hackers. "Egos and machismo tend to cloud the reason we got involved in the first place," we said. They also prove to be fatal if we are trying to justify our existence to the authorities. It doesn't take a genius to figure this out.

By creating the appearance of warring factions, we give the media permission to turn it into reality. Once they do this, it no longer matters whether or not it was ever true to begin with. It becomes the truth.

While we have no doubt that there was childish mischief going on at some point, to claim that it was part of a carefully coordinated conspiracy is a gross distortion. Sure, such a claim will get attention and will probably result in all kinds of charges being filed. Lives will be scarred, headlines will be written, and a lot of time and money will be wasted. Is this the only response we're capable of coming up with when people act like idiots? If so, then we've just made the government's job a lot easier.

here they are

Trouble To Come

Dear 2600:

I've found a bug in all versions of VMS to date! First, some background on SYSGEN. SYSGEN (SYStem GENeration utility) is a program that allows properly privileged accounts to modify fundamental system parameters.

Any user, no matter what privileges he possesses, can run the SYS$SYSTEM:SYSGEN utility, but without proper privilege to access SYSGEN's data file (SYS$SYSTEM:VAXVMSSYS.PAR), actual changes are never made.

Here's the bug: if a user goes into SYSGEN and performs the WRITE CURRENT command, an OPCOM security audit alarm goes off telling the system manager that "Current system parameters have been modified by process XXXXX", even when parameters aren't changed for lack of privilege!

Obviously, this is a good way to freak out your system manager. The manager of the system I tried it on nearly had a heart attack when he thought I had given myself privs and changed the parameters, since there is usually no written record of what parameters are set to.

Maelstrom 517

Enhanced Exaggerations

Dear 2600:

You might have seen a television advertisement from Bell Atlantic promoting their package of optional features, namely Call Waiting, Call Return, and Caller ID.

The basic story of the commercial is that a husband at work calls up his very pregnant wife who can't make it to the phone before he hangs up. But no problem, she has Call Return so the phone will "remember" and return the call. And he, at work, has Caller ID so he knows it's her calling.

An hour later, she starts having labor pains and calls him again. He can't leave work, so he calls a friend (thanks to Call Waiting which "lets important calls get through"). Interestingly, there are two versions of the commercial at this point - one of them simply has the friend calling out. The other has a voice-over which says "Tone Block" keeps anyone from interrupting your important calls.

At the end, husband and wife are in the hospital with new infant, and they get an incoming call from their friend who used Call Return to get back to them. However, if you think about it, in most cases hospital PBX's will not send out a "proper" ANI. (Nor, for that matter, would other businesses.)

Danny
New York

It's not the first time that phone companies have resorted to lies and deception to make a quick buck. It won't be the last.

Mag Strip Update

Dear 2600:

I have a few updates about the letter from Mr. Upsetter about the Taltek 727 as it was partially incorrect. He must have had a template taped/glued onto the front of his Taltek keypad, therefore all standard non-templated Talteks will not have the same keys. Also, not all Taltek 727's are endowed with a "calculator mode."

What I might add that could be helpful to some mag-strip hackers is that some of the used units have the numbers of credit card companies' verifier numbers stored in their "password protected area." But unfortunately, you can't access this the same way on every Taltek. Not only that, but the password is different from machine to machine. If you do access it, however, be sure to monitor the extension and record anything that goes between the modems. If anyone knows of a DIN-5 serial to 25 or 8 pin serial converter, tell about it. That way, the machine can be hooked up to PC's for easier monitoring (and future mag-strip editing?).

SE
Minnesota

Scanning Results

Dear 2600:

Here are a few things I have been wondering about for a while, and I was hoping you could enlighten me. All of these observations are valid for the Atlanta, Georgia area code (404).

1. When I dial any number with certain prefixes, I always get a busy signal before I even hear a ring. It does not seem to matter which number I dial. Examples: 450-XXXX, 470-XXXX, 490-XXXX, and 670-XXXX.

2. One prefix always returns a fast busy signal (which I believe is the local reorder tone). This tone pops up after you dial the first three digits of the prefix (no additional digits necessary). Example: 430.

3. For some prefixes, you dial a full seven digit number and then you get exactly one ring and then a series of three or so single frequency beeps. Examples: 570-XXXX and 690-XXXX. In some extremely rare cases you will get something like an answering machine service after the first ring. The announcements are made by real people, and vary from number to number.

4. Some prefixes require that you enter a number consisting of ten digits. After the second or third ring an announcement comes up and says something to the effect of: "Your call cannot be completed as dialed. Please read the instruction card and try again." Examples: 510-XXXX-XXX and 410 XXXX-XXX

Since I have not made any progress figuring out any of the above stuff, I decided to see if you could help me out. Any information you can provide will earn you my everlasting gratitude. And if you cannot help, that's OK - I will still keep reading 2600 Magazine whenever I can lay my grubby hands on a new issue. I apologize in advance if any of this stuff has some simple explanation that has been common knowledge for years.

FD
Atlanta

First off, never apologize for wanting to learn. It's far better to admit ignorance than to feign knowledge. And since 99 percent of the populace have no idea what we're talking about anyway, you're still coming out ahead.

We checked with the AT&T routing computer and all of the exchanges that you were getting busy signals on (450, 470, 490, 670) are not officially in use. They also cannot be accessed from outside the 404 area code. This could mean several things. These may be new exchanges that are still being tested. They may be special exchanges that the phone company uses for various things. We suggest exploring each of these exchanges every now and then to see if all of the numbers remain busy. Also, it can't hurt to have a local operator check the busy signal and tell you if the line actually exists.

Some exchanges (like your 430) are programmed not to accept any additional digits. It's more likely that this exchange is not being used at all in your area. To be sure, though, compare it to other exchanges that are not being used. Weird numbers like 311 are almost never used but so are a lot of other three digit combinations. Do they all react the same way? Keep a log and compare it every few months.

The 570 and 690 exchanges in your area are used for beeper services. When you get one ring followed by three or four beeps then silence, you have dialed someone's beeper number and it is waiting for touch tone input from you. When you dial a sequence of numbers followed by the # key (optional), those numbers will show up on the beeper belonging to that number. If you get six or seven beeps that don't ever allow for touch tone input, you've reached what is known as a "tone only" number. The beeper will simply say that someone beeped but won't give any additional information. This is seldom used these days and is good only for people who get beeped by the same number exclusively (i.e., doctors who get beeped by their service). When you hear a voice message, you're reaching a service that is attached to someone's beeper. When you leave a voice message of your own, their beeper will go off telling them they have a voice message in their mailbox. Some of these numbers allow for either tone or voice messages to be left

Since 510 and 410 are now area codes, this would explain why your switch waited for seven more digits.

On all of these numbers, we suggest you try prefixing with 1 or 0 or a carrier access code to check for variations. And we encourage people in different area codes to experiment in the same way and report their findings here

Dear 2600:

Here are a couple of modem phone numbers a friend stumbled upon and passed on to me. I haven't been able to make them do anything, but I thought I'd share them:

315-472-0183 - rings into some kind of NYNEX computer.

703-684-5772 - gives you a choice of four destinations.

Good luck.

Name Withheld
Address Withheld

These are interesting numbers. The second one has four destinations known as VENUS, MARS, HERMES, and ZEUS. ZEUS appears to be running on a PDP-10, a machine many hackers got their start on.

Dear 2600:

Did you know the Software Piracy Association has a toll-free number that connects to a voice mail system after hours? The number is 800-388-7478 and it's used to turn in people who are committing software piracy.

David

Any group that encourages people to rat on each other over voice mail speaks volumes as to their intelligence. This organization also sells a video called "It's Just Not Worth The Risk." If you know somebody who's pirating the video, there's probably another number to call.

At Wit's End

Dear 2600:

I have spoken with college telephone administrative assistants. I've called AT&T technicians. None have answered my questions. Now it's time to speak to the experts.

As a college administrator at a small school in Colorado, one of my responsibilities involves responding to students who are victims of harassing phone calls. This past school year has seen a drastic increase in the kind of heinous phone calls that put college women in fear for their lives. (We're not talking about cute prank calls here.)

Here is the technical background: The college phone system works around its own PBX allowing "on-campus" calls to be dialed with only four digits. Calls to phones outside the PBX require a "9" to "get out."

The college phone system has voice mail as an option. The voice mail system not only records the caller's message, but also tells the date, time, and most importantly it records the caller's extension if the call is from on-campus.

The question: I want to catch the caller(s). Doesn't it make sense to you that since the voice mail system is able to record the caller's extension if he/she leaves a message, that there is a way to note the caller's extension if the "callee" answers? Suggestions?

Of course, a technically savvy caller could dial 9 to get off campus and then call his/her victim by dialing all seven numbers. The voice mail system is only able to note that the call is coming from "off-campus." This leads me to my second question: There are apparently 50 lines into the college's PBX. I am told that the only way we can know the source of a call is to have "phone traps" placed on all 50 lines, and then find the source by matching the time of call. What do you think?

ANI is not an option for the near future; legislative and corporate hang-ups are still clogging up the system.

2600 is by far my favorite 'zine. Keep up the good work.

CB
Colorado

Your system sounds like a ROLM. Whether or not it is, the same logic will apply. First off, it's possible to block the 9+ feature to the college, especially if your college owns the entire prefix. If not, individual numbers can be blocked in this manner. It's also possible to log all calls that are made in this fashion. But, more importantly, your telecommunications department needs to be more up front with you. Don't settle for assistants; speak to whoever's in charge. Obviously, if the voice mail system is receiving information on which extension is calling it, the capability exists for that to occur on non voice mail calls. It's only a matter of setting it up. There are special display phones on most systems that show this information on a screen. (On ROLM systems, they're known as 400's.) We suggest attaching one of these onto the lines that have the problems. As for as anything coming from off campus, you will need cooperation from the local phone company. We'd be extremely surprised if they weren't using ANI in this day and age.

If all else fails, try forwarding the problem lines directly to a voice mail message that sounds as if a real person is picking up. This may trick the caller into leaving a message thinking they're speaking with a person. Then if they're on campus, you'll have the number. And if that doesn't work, try to trick them into calling something that WILL log their number, like an 800 number.

crypt( ) Correction

Dear 2600:

A couple of months ago I purchased the Winter 1991-92 issue of *2600 Magazine*, primarily because I was interested in the source for the crypt( ) function, which was contained in it.

Only recently have I had time to seriously look at it, and I have discovered the following flaw in my copy of the magazine.

On page 14, there is an array: char S[8][64] of "selection functions", which consists of eight blocks each containing 64 character values. In my copy, the first line of the last of these eight blocks is partially distorted. The line consists of 16 numbers, but the second and third numbers are not readable in my copy.

What I can read is: 13, ??, ??, 4, 6, 15, 11, and so on.

What are these two missing numbers? If someone can check another copy of the magazine and drop me a line to let me know what they are, I would be extremely grateful.

SJ
California

Unfortunately, all of the issues have the same printing defect. The numbers should read, 13, 2, 8, 4, 6, 15, 11, etc. We're sorry for any inconvenience.

Simplex Sightings

Dear 2600:

The University of The District of Columbia (UDC in Washington, DC) has a load of Simplex locks on their campus. Just letting you know since I didn't see it listed in the Spring 1992 issue.

Albatross

Thanks for the info. As we are all beginning to see, these locks are everywhere. We welcome pictures of supposedly secure areas that use these as the only form of protection.

Wanted

Dear 2600:

I have recently purchased your magazine and I like what I see. I don't have a computer yet, but I am interested in obtaining programs on disk that can copy application programs from a hard disk drive and/or floppy disks such as WordPerfect 5.1, PageMaker, and Corel Draw, even if they are under someone's homemade menu screen, under Windows, or both. Also, I would like information on telephone codes to make free long distance calls (and any other phone tricks), a program to find the source code for any IBM compatible computer, and some type of beginner's guide on hacking that isn't technical. I was wondering could you tell me which back issues of 2600 deal with these subjects and could you give me a list of other sources - magazines, books, or people (addresses and phone numbers) that would have what I am looking for. I would greatly appreciate it. Keep up the good work.

Bledman
Tennessee

Learning is a lot more fun and beneficial than making free phone calls and copying software. While the things we teach may enable people to accomplish these tasks, we believe they will at least understand what it is they are doing. You seem to want to bypass this part of it and that's something we cannot help you with. If, though, you're interested in more than just the end result, then you're in the right place.

Monitoring Problems

Dear 2600:

I just recently picked up a copy of your magazine. I really do like the information it offers, although some of the things you print are a little above my head. I would like to learn more about phone phreaking just for the fun of knowing. After all, isn't knowledge power? Anyways, I tested the mobile phone frequencies for Minneapolis/St. Paul. I heard the tone you mentioned but then at times my scanner went blank. All I heard was white noise! Can you tell me what I was doing wrong? I am also interested in creating a computer network to cut down on the cost that is incurred when calling BBS's across the nation. I am wondering if you could help me out. I need information on how computers can send information over radio waves. I want to set up a computer station in every area code that can be accessed by radio. I would also like to know if maybe your readers might be interested in helping out. I would also like to set up a computer on that network for 2600 readers to send feedback and other things of that nature to other readers of your magazine.

Vid Kid
Minnesota

Your goals are indeed admirable. You need to speak to some ham radio people concerning *the project you're interested in. We would also suggest reading Popular Communications and Monitoring Times. If any of our readers have suggestions, we'll pass them along.*

As to the problems you had with your scanner, some IMTS systems use a form of frequency hopping, similar to cellular frequency hopping. Not all IMTS systems do this but it's possible the one in your area does. We suggest you go into search mode for the entire range of IMTS frequencies and you should be able to catch up to the original conversation.

Cellular Frequencies

Dear 2600:

This may not be of much interest to you in the U.S., but I came by a list of frequencies for the U.K. cellular/cordless phone system. The cordless phones can be picked up with a re-tuned medium wave radio by hanging out on the base frequency, which seems to transmit both sides of the call. The cellular ones need two separate receivers.

These are cordless phone frequencies in the order of: channel number, base unit transmit frequency, handheld unit frequency:

1, 1642.00 kHz (1.642 MHz), 47.45625 MHz; 2, 1662.00, 47.46875; 3, 1682.00, 47.48125; 4, 1702.00, 47.49375; 5, 1722.00, 47.50625; 6, 1742.00, 47.51875; 7, 1762.00, 47.53125 or 47.44375; 8, 1782.00, 47.54375.

These are cellular phone frequencies in the order of: channel number, transmit frequency, duplex split, receive frequency:

301, 897.5125 MHz, 45 MHz, 942.5125 MHz; 302, 897.5375, 45, 942.5375; 303, 897.5625, 45, 942.5625; etc. at 25 Khz spacing until: 599, 904.9625, 45, 949.9625; 600, 904.9875, 45, 949.9875.

6025
Scotland

What the NSA Does

Dear 2600:

Congrats on a cool magazine. Liked the article on Crypt(). Got into a discussion with one of the guys at work who used to work at NSA. Said several neat things:

1. The original keys for DES were supposed to be 128 bits. NSA ordered the change to 56 bits because they CAN break 56 bits.

2. UNIX crypt() is hobbled in an additional way (he wasn't sure but it had something to do with re-use of keys).

3. These guys have their own chip foundry in a (no shit) copper walled building.

4. They go after and change other people's encryption standards. A couple of years back IBM was going to come out with a real good one and NSA forced them to shelve it.

5. The tables in DES were generated by the NSA with the intent that they could break it.

If you want to print any of this, please don't print my name. My friend says that these guys are very paranoid and so am I!

I'd like to see some magazine come out with a public encryption standard, but I wouldn't want to see you guys do it, because the NSA would shut you down.

Be careful with this stuff, because those NSA dudes scare me.

Someone
Somewhere

We altered your name and town. Is that careful enough?

Prisoner News

Dear 2600:

Many greetings from the gulag. In recent months I've noticed more and more letters and such from imprisoned hackers. Another prisoner and I edit and publish a monthly newsletter called *Prisoners' Legal News*. People can get a free sample copy of *PLN* by writing to our publisher at: *PLN*, PO Box 1684, Lake Worth, FL 33460.

Apart from organizing against the state parole board, we have been lobbying hard for the state to allow prisoners to have PC's in their cells. For three years, prisoners at a state prison had PC's in their cells. All PC owners who got released have gotten jobs and none have returned to prison. There were no security or other problems but in an arbitrary decision, prison officials made prisoners send the PC's out.

PW
Washington

What you witnessed was the typical panic reaction that authority figures have shown towards technology. Their ignorance frightens them and annoys the rest of us. We wish you luck and hope you keep us updated.

Mystery Calls

Dear 2600:

I have just picked up my first issue and I really like what I see. I don't consider myself to be a great hacker, but I do have some very basic electronic skills and some fairly extensive programming skills.

Recently, while I was flipping through the UHF channels, I picked up a very interesting phenomenon: phone conversations. My TV doesn't normally receive UHF channels, in fact, there isn't even an antenna hooked up to the UHF input, only VHF. My TV is a fairly old (very early 80's) model. It has a rotary knob for VHF and UHF, plus individual tuning rings on the outside of both knobs.

I have noted that there are as many as four conversations at a time and they seem to be in my neighborhood. They only appear at the very end of the dial, around channel 83, however it requires a lot of tuning to even get it with a lot of static. If I get lucky, it sounds as clear as if you were on an extension! After one person hangs up, the signal jumps and I end up having to retune it.

About the only possibility I've been able to come up with is that the shielding is ineffective on our neighborhood connection post at the edge of the street by my house.

Now I have heard stories about people getting images on monitors from others due to RF interference. In fact, our beloved government was in a panic over this issue not long ago. What I would like is your opinion about this phone interference. Also, could you tell me what the frequencies in this area are and if I could get ahold of some kind of radio equipment that could receive these frequencies?

Sitting Duck

What you're experiencing has nothing to do with ineffective shielding. The upper UHF channels on older TV sets happen to cover the same frequencies that are now used for cellular telephones! And every time you listened in, you were breaking a federal law. That is the extent of "protection" that is given to cellular phone calls. You can buy a scanner that covers the 800 Mhz spectrum which is where cellular calls can be found. Buying such a scanner is legal. Owning one is legal. Listening to those frequencies is illegal. By the way, if anyone happens to tape any broadcasts over those public airwaves, please send them to us. We promise not to listen. (Make sure you don't either.)

The Prodigy Side

Dear 2600:

I know I'm treading on thin ice voicing a corporate viewpoint in 2600. But I think it's important to clear the air regarding Prodigy.

There have been a lot of rumors about Prodigy and STAGE.DAT, and what we're doing - and not doing - with our members' data and computers. Prodigy doesn't read, upload, or interact in any way with a member's file on their computer. The sole exception is Prodigy files. There's no way we could or would do the kind of things Big Al alleged in your Autumn 1991 issue, and that were discussed in the letters column in the Winter 1991-92 issue.

The confusion and false claims arose because non-Prodigy data found its way incidentally into Prodigy files. When people saw this, they incorrectly assumed Prodigy had delibererately sought this information and uploaded it. In fact, any non-Prodigy data found in Prodigy files was incorporated randomly because of two programming shortcuts that have since been eliminated. None of it was ever looked at, manipulated, or uploaded by Prodigy.

The two Prodigy files in question are STAGE.DAT and CACHE.DAT. STAGE.DAT stores Prodigy programs and graphics between sessions. Without STAGE.DAT, all of this data would have to be transmitted every time the member moves from place to place within the service or "turns a page".

CACHE.DAT stores Prodigy content for reuse within a session so that the member can move from feature to feature without retransmission of content already sent. CACHE.DAT is overwritten during each session.

During the offline process of installing the Prodigy software, STAGE.DAT is created as a file either 0.25 or 1 megabytes in size, whichever the member chooses. As with any new file, when it is created DOS allocates disk sectors to it. It is well known that those sectors may include the contents of previously erased files, since DOS doesn't actually erase information contained in erased files, but simply recycles the space for use in new files.

Earlier versions of the Prodigy software did not zero out the file space allocated to STAGE.DAT. The result was that if you used XTree or DEBUG you might have noticed that, prior to being filled with Prodigy data, STAGE.DAT disk space contained information from erased files. A similar effect occurs with the smaller file, CACHE.DAT.

After the STAGE.DAT file is created, the installation program builds a table of the entries in it. This table allows the STAGE.DAT to keep track of the programs and graphics stored there. The software creates this table in RAM (memory) and then moves it to the STAGE.DAT on the disk. As a backup, we even write two copies of the table to the STAGE.DAT on the disk. As a backup, we even write two copies of the table to the STAGE.DAT, so there are two places where a member might see this information. We move the whole portion of RAM used for the table, even though it may be only partially filled with entries. Again, we didn't zero the RAM space used to build the table, so any memory that wasn't written over - and its contents - was swept into STAGE.DAT.

Our programmers originally wanted to make installation as fast as possible, and so they did not want to take the additional time to zero out disk sectors or memory involved in the installation.

During a Prodigy session, calls on RAM buffers are used to write new graphics and program data to the STAGE.DAT file. In the earlier versions of the software, the buffers were not zeroed, and the amount of Prodigy data stored in them may not have completely displaced data already in the buffer memory area from earlier programs. Then, when the Prodigy data is written to STAGE.DAT the other information would also be transferred to the disk. That is the reason Big Al saw fragments from his Wordstar files in STAGE.DAT.

The personal information was of no interest to Prodigy, and in any case, over time, this information is overwritten as programs and graphics are added to the STAGE.DAT file during use. We have since learned of our members' sensitivity on this issue, and have modified our software accordingly. For people with older Prodigy software, we provide a free utility program that zeroes out all non-Prodigy information for existing STAGE.DAT and CACHE.DAT files. To order it, JUMP TECH TALK on Prodigy.

We never looked at or used any non-Prodigy information in STAGE.DAT or CACHE.DAT. There is, in fact, no mechanism that would allow the Prodigy software to pass any information (Prodigy or non-Prodigy) contained in the STAGE.DAT or CACHE.DAT files up to the host.

To help put the rumors to rest, we asked the national accounting firm, Coopers and Lybrand, to audit our operations. They examined Prodigy's computers and files and interviewed our employees for six weeks and found that we did not upload any non-Prodigy data.

As far as Big Al's allegation that he received Prodigy direct mail solicitations sent to dummy names from a LAN he uses, I don't believe it. The names on mailing lists Prodigy uses for direct mail come from lists supplied by magazine subscriptions, computer catalogers, and so on. If Big Al thinks he's got grounds for complaint, we'd be happy to look at the direct mail pieces he got from Prodigy and see where the names came from.

One final point. Big Al mentioned in his letter that Prodigy requires a "loaded" PC or Mac. The truth is just the opposite. Prodigy has taken care to ensure that the service will run on very basic DOS or Mac machines, such as an XT with an 8088 and 540 Kbytes. After all, our service is aimed at the home market. That's why we've designed it to run on the kind of machines people have at home - as well as the ones they might use in the office.

If Big Al or any other readers want to call and discuss this, my number is 914-993-8789. Or send me a message on Prodigy at PGPI97a.

Steve Hein
The Prodigy Service
White Plains, NY

Going under the assumption that everything you say is true, there are still two disturbing facts that we have maintained from the beginning. First, if Prodigy did not respect the privacy of its users, it would not be too difficult to do everything that has been suggested. Perhaps other companies will do this in the future. Perhaps some already have. It's a possibility that cannot be ignored and we're glad the issue has come up, regardless of Prodigy's actual involvement. The other fact is that Prodigy was given a fair chance to express its side of the story from the beginning. Nobody seized all of your equipment to investigate the matter. The media didn't label you as potential terrorists. You were never threatened with decades of prison time for a crime nobody really understands. We find it sad that individuals automatically mean so much less than large corporations when their integrity comes into question.

HOW TO DEFEAT *69

by Bernie S.

It's annoying! You call someone and, for whatever reason, you'd like to protect your telephone privacy. In other words, you don't want them calling you. But with new telephone services like Return Call (*69), they can call you back as often as they like until someone else calls them. If they have Caller ID it's even worse, it will tell them your telephone number and they can call you whenever and as often as they like.

Many people feel this is an invasion of their privacy. People who pay extra for unpublished numbers are just as vulnerable. The Bell Operating Companies reap huge profits from the use of these services, but seem insensitive to the concerns of customers who want to preserve their telephone privacy. There are methods of overcoming this problem, but the phone companies refuse to publicize them because they could lose out on many millions of dollars in new revenue if services like Return Call and Caller ID aren't widely accepted.

This article describes several methods you can use to defeat Return Call (*69) and Caller ID so that you can use your telephone without fear of compromising your telephone privacy. Most of these techniques will work in different parts of the country, assuming the services are available in the first place. It is possible that your area uses different codes for these services. If so, please tell us what they are.

Calling Card Method

This method defeats both *69 and Caller ID. To use it, you need a valid calling card from your local company. You can get one by calling your local business office.

Dial 0 plus the area code and number you're calling. After the "bong" tone, enter your calling card number and your call will go through. If you're calling from a dial or pulse-type phone, stay on the line and tell your calling card number to the operator who answers. If the operator asks why you're not dialing direct because it's cheaper, tell them to just complete the call anyway. The surcharge for this is about 40 cents and will vary depending upon what part of the country you're in.

Operator Assisted Method

This method defeats both *69 and Caller ID and does not require a calling card. Dial 0 plus the area code and number you're calling. After the "bong" tone, dial 0 or wait and an operator will come on the line. Tell the operator that you'd like this call billed to the number you're calling from. If the operator asks why you're not dialing direct because it's cheaper, tell them to just complete the call anyway. The surcharge for this is about $1.50.

Long Distance Carrier Method

This method defeats both *69 and Caller ID and requires a long distance calling card. Follow the instructions on your calling card for making a call, but dial the local number you want to call as if it were long distance, i.e. include the area code. If you don't have a long distance calling card, just request one from the company of your choice, the vast majority of which are listed with 800 information.

When you call to request your calling card, they will try like hell to get you to make them your primary long distance carrier. If you don't want to switch, just say so and explain that you'd like one of their calling cards anyway. Since there's no fee for a calling card, you might as well collect them all! It's a good idea to have calling cards from several different long distance carriers so you can compare their rates and service quality.

You will be billed according to the rates of the long distance carrier you're using. Rates for calls within your area code are lower than interstate long distance calls. Call the long distance carrier's customer service number for exact rate information.

Most calling cards have surcharges. If at all possible, use a company that has a non-surcharge 950 access number. Metromedia Long Distance (formerly ITT) and Cable & Wireless both offer this service but give it out sparingly.

As with the above methods, if someone dials *69 after your call they will hear a recording that says "the number is not in the serving area." A Caller ID unit will display "Out of Area."

Answering Machine Hang-up Method

This "quick and dirty" method is effective in defeating *69 call backs in response to your leaving a message on an answering machine. After you've completed a call to an answering machine at the number you desire privacy from, hang up and immediately call again using one of the above methods.

The moment you hear a ringing signal through your handset, *hang up*. When the called party returns home and gets your message, any *69 attempt will generate a "number is not in the serving area" message. If you hang up the second time before their machine answers, you won't be charged for that call. This technique does *not* work well when calling people who are home, because they'll usually be able to dial *69 before you can call the second time.

Call Block Method

This method prevents others from using *69 (1169 pulse) to call you back by blocking selected telephone numbers in your area code from reaching your line. It does not prevent Caller ID *from* revealing your telephone number.

Before you make your call, you must *block* the specific telephone number(s) you're planning to call from being able to call you back. To do this, dial *60 (1160 pulse) then # (12 pulse) and enter the telephone number(s) you wish to block. After you enter each number to be blocked, enter # (12 pulse) again. You can block up to six numbers at a time and you can block calls from the number you just received a call from by entering 01 in its place.

To remove individual numbers from your blocking list, enter * (11 pulse), the number you want to unblock, and * (11 pulse) again. Hang up when you're finished.

When callers whose telephone numbers are on your blocking list call you, they'll hear a recording that says, "At this time, the party you have called is not taking calls." However, the called party will still be able to use *69 to call you back *after* you unblock their number if they haven't received any calls since yours. One way to rectify this problem is to use the "Answering Machine Hang-up Method" *just before* deactivating Call Block.

Call Block costs about 50 cents *each day* it's left on or around $5.00 per month for unlimited usage. If you're not subscribing to it on a monthly basis, don't forget to deactivate it when you don't need it or it could end up costing you over three times the monthly rate. To deactivate Call Block, dial *80 (1180 pulse), then enter 08 and hang up.

Select Forward Method

This method prevents others from using *69 to call you back from up to six telephone numbers that you select. It forwards those calls to any other number in your area code.

To accomplish this, dial *63 (1163 pulse), then 3. After the tone, enter the telephone number you want calls forwarded *to* and then # (12 pulse). When prompted, enter 1 and then # (12 pulse) when prompted again. Next, enter the telephone number(s) you wish to have calls forwarded *from*, with a # (12 pulse) after each number. You can forward calls from the number you just received a call from by entering 01 in its place. Hang up when you're done.

Select Forward costs about 50 cents *each day* it's left on or $3.50 per month for unlimited usage. If you're not a monthly Select Forward subscriber, don't forget to deactivate it when you don't need it or it could end up costing you over four times the monthly rate. To deactivate Select Forward, dial *83 (1163 pulse), then enter 08 and hang up.

Ultra Forward Method

This method defeats both *69 and Caller ID, but you must have an auxiliary telephone line that you don't care about the privacy of, and Ultra Forward service. The additional line can be your business number at another location, but you must have billing responsibility for that line to be able to request the Ultra Forward service.

The idea here is to remotely program your auxiliary number to forward calls to the number you want to call, and to call that auxiliary number whenever you want to reach the number you desire privacy from. If the called party dials *69 after you call them, they'll get the auxiliary number instead of the number you called from. If the Ultra Forwarding is still on, it will call back their own number, give them a busy signal, and charge them for the *69 attempt! A Caller ID unit will display your auxiliary number, *not* the "private" number you called from.

To accomplish all this, call your business office and request Ultra Forward for your auxiliary line. This new service costs around $5.00 a month.

You must remember to deactivate the Ultra Forwarding, or else any other calls actually intended for the auxiliary number will also be forwarded to the number you desire privacy from. If you have calls forwarded to a long distance number, you will be billed for the long distance charges whenever calls are forwarded there.

Hardware Forwarding Method

This method is similar to using Ultra Forward, except that you connect a special device between two auxiliary lines. This accomplishes the same job without having to pay the phone company's monthly charges. Call forwarding devices are available from Radio Shack and similar stores for about $100. Specific model instructions vary, so read your owner's manual for details.

Cellular Phone Method

This method stops *69 and Caller ID, but it requires a cellular telephone. Return Call and Caller ID do *not* work through cellular telephone exchanges. Anyone dialing *69 after receiving a call from a cellular telephone will hear a recording that says "The number is not in the serving area." A Caller ID unit will display an "Out of Area" message.

Most cellular phones are installed in vehicles, but transportable and hand-held models are rapidly becoming more popular and less expensive. The cost of a call varies depending on if it's during the day, evening, or weekend and its duration. Call your local cellular carrier for information about cellular phones and rate plans.

Payphone Method

This is certainly the least convenient method, but it does stop *69 and Caller ID users from compromising your privacy. If you make calls to those parties from a payphone, your home telephone privacy will be ensured. If you don't have change, you can use a calling card, but it will cost more. The best and least-expensive payphones are generally those owned and operated by the Bell Telephone company serving your area.

Creative Techniques

If you're creative you can confuse and defeat the most determined unwanted callers. For instance, you can use Select Forward to send someone's calls back to their own number so they'll always get a busy signal whenever they call you. As mentioned above, this also works if they dial *69 after you call them, and as an added bonus they'll be billed for the attempt!

Another trick is to have calls from selected unwanted callers forwarded to the police, to a non-working number, to a payphone, or to some other person who's also insensitive to your privacy. If the second party dials *69 after your unwanted caller hangs up, it will call back that number, not yours. Caller ID units will also display their number, not yours.

Call Trace: The Real Story

Many phone companies advertise Call Trace (*57) as a convenient way to trace annoying or harassing calls so you can put a stop to them. The truth is, they make it very difficult and expensive for customers to accomplish this. When you dial *57 after receiving a call, the phone company's computers record the calling number, your number, the date, time, and duration of the call and sends all of this to their Annoyance Call Bureau. The phone companies also charge you on the order of $1.50 *every time* you dial *57.

Despite this, the phone company will not even consider any traced calls worthy of their attention until you have successfully traced six such calls from the same originating number! This means if your unwanted caller is calling from payphones or more than one location, you could end up paying quite a lot until the phone company determines that you've traced six "qualifying" calls.

Once they are satisfied that you've traced at least six calls from the same calling number, they'll mail you a legal release to sign and return to them. This release prevents you from suing them, and *grants them permission to tell the unwanted caller your name and telephone number* (ostensibly so that the phone company can justify a request to ask them to stop). It also states that the phone company will *not* tell you who is harassing you, which seems rather sleazy in light of the fact that they're willing to sell Caller ID-type services to anyone willing to pay $6.50 a month for it.

If you don't want them giving your name to this person, you should cross out the section of the legal release that gives them permission to, and also cross out the section that releases them from liability (thus protecting your rights). Initial and date the changes and attach a signed letter demanding that they not violate your privacy by releasing your name to the unwanted caller. Also demand that they promptly turn over all evidence of your telephone harassment to your local police department.

For maximum impact, you can further mention that if they fail to comply with your request, you will file a complaint against them with the State Public Utilities Commission. All local phone companies are extremely sensitive about this and it's almost guaranteed to get fast results.

Send your letter and the amended release back to their Annoyance Call Bureau via certified mail (return receipt requested) and your local police should call you in a few days. If not, call them and ask if the phone company sent the information. If so, diplomatically ask them who is harassing you (promising not to take the law into your own hands) and they'll usually tell you.

If the calls persist, press charges against the caller for "harassment by communication." Police departments are being inundated with Call Trace requests and they generally want to resolve these cases as quickly and as easily as possible. The phone companies only seem to be interested in protecting themselves - at your expense.

More Telephone Privacy Tips

Most toll-free 800 numbers receive ANI (Automatic Number Identification), which gives them the phone numbers of most of the people who call them. It's not the same as Caller ID but it can have the same effect. Apart from seeing these phone numbers when they get their 800 bill, these companies can use equipment that allows them to see the numbers immediately. Whether you call a TV shopping channel, a mail order company, a drug or health-related hotline, or a TV ad selling Elvis music, almost any company with a toll free 800 number you call can learn your telephone number the moment they answer your call. This makes you vulnerable to having your telephone number listed and sold to other telemarketing companies. Ready buyers include companies that may employ sleazy salespeople or those annoying automatic selling machines that are programmed to call everyone who's ever responded to a particular type of sales pitch before.

Moreover, telephone companies sell computerized directories to mail order firms, telemarketing companies, and credit bureaus, which cross-reference the telephone numbers to get names and addresses. Purchasing records are cross-referenced to determine people's buying patterns for certain types of products, services, and financial transactions. Many companies buy and sell this information for a living. Ever wonder how you got on all those mailing lists?

You can safeguard yourself against this type of telephone privacy invasion by making your toll-free 800 calls from a cellular or pay telephone or by using the Ultra Forward or hardware call forwarding methods. (Having the operator place your toll free call will also keep your number from being displayed.) You should *always* decline to give your telephone number out to any person, company, or organization you don't want to have it.

Unlisted Numbers are not really all that private. According to the *Philadelphia Inquirer* and other publications, phone companies provide special directories to police departments and certain government agencies that contain *complete* alphabetical listings, regardless of their "unlisted" status. Even worse, the phone companies have repeatedly been accused of giving out confidential customer information to select individuals, private investigators, and to police without warrants. So if you *really* want to keep your name, address, telephone number, and calling records out of the hands of others, you should consider getting a new telephone number put in a different name.

Emergency 911 services in many areas now employ a special system that instantly displays the caller's telephone number, name, and address. Anonymous calls to 911 can only be ensured by calling from a payphone.

Reverse Directories of telephone numbers and street addresses with names and approximate household incomes (with phone numbers and street addresses listed numerically) are published by several companies, including Cole Publishing, Inc. These directories are very popular with real estate companies, telemarketing firms, police departments, or anyone else wanting to know more about people. You can write to Cole Publishing and request to be omitted from their directory. They have offices throughout the country.

Unsolicited Telephone Sales Calls to your number can supposedly be reduced by writing to the Direct Marketing Association. They will put your name, address, and telephone number on a list distributed to telemarketing firms, which are then legally required to stop calling you. Their address is: Direct Marketing Association, Telephone Preference Service, 11 West 42nd Street, Box 3861, New York, NY 10163-3861. Provide your full name, address, and telephone number(s) and request to be put on their "No Contact" list. Of course, just doing that does put you on another list...

demon dialer review

(continued from page 17)

Blue Box a particular number, wait until a key is pressed, play another macro, wait until a key is pressed, and then retry. The mode is extremely flexible and easy to use. The Dialer can store up to 10 different macros, even after the device powers down.

The user programmable mode is by far the most powerful feature of the Dialer. This mode gives you total control, allowing you to program a series of any tones and pauses you want. You choose the number of tones (zero, one, or two), the duration of each tone (in milliseconds, up to one second), and the volume level of each tone (from 0 to -15 dB of full volume) for up to 22 keys (you get the extra keys by using the shift key). You can also define the timing type so that your program is played-while-pressed. This is the mode that makes the Demon Dialer a true Rainbow Box. We programmed a North American dial tone, busy signal, fast busy, and off hook signal with no problems.

The Dialer also offers some other features called Special Functions. These include a device initialization (clears the RAM), RAM FIN programming, time template programming, guard tone programming, frequency stepping, continuous sweep, password protection on/off, number scan, and power off.

We Approve

The $250 price tag of the Hack-Tic Demon Dialer is stiff, especially considering that it lacks a chassis and does not even come assembled. However, a few facts should be kept in mind before we judge the Dialer as a nice but overpriced toy.

First of all, to call the device a "dialer" at all is really a misnomer; it is a computer complete with its own CPU, ROM, and RAM. Although it may not seem like a computer because the output is audio and not video, it is still quite capable of performing amazing feats considering its size.

Secondly, because the Dialer is programmable, we cannot even begin to list what it is ultimately capable of. With a little imagination, the Dialer would be excellent for social engineering. We have not had the time to fully explore its practical uses, but we will welcome ideas and suggestions from our readers.

Finally, the Dialer is one of a kind in terms of its capabilities. Hack-Tic did not design this device to sell it; they are hackers and designed this device to use. You can therefore be assured that they are not holding back on anything. As further proof of this, the software that came with the original Dialers has since been updated.

We at *2600* would like to see the price go down not because the Dialer is overpriced, but because the high price is steep for many hackers, and therefore makes the Dialer exclusive. We would ultimately like to see the technology available to everyone, as it is truly a tool of exploration and not just another box to defraud phone companies.

If you are considering purchasing the Dialer, but are not sure whether it is worth it, then consider that it is ultimately a phone phreaker's tool. Those who come into contact with phones and phone equipment on a regular basis will find the Dialer to be invaluable. Because it is designed to handle phone systems around the world, frequent travellers will also find the device to be an invaluable companion, and will use it to its full potential. If all you are looking for is a red box to defraud your local payphone, then you may want to look elsewhere. On the other hand, if you are searching for the phone phreaker's equivalent of an all-terrain vehicle, then you just may want to test drive this rocket.

Bellcore

[illegible]

Leonard Charles Suchyta
[illegible]
[illegible]

LCC 2E-311
290 W. Mt. Pleasant Avenue
Livingston, NJ 07039
[illegible]

CERTIFIED MAIL - RETURN RECEIPT REQUESTED

July 1, 1992

Emanuel Golstein, Editor
2600 Magazine
P.O. Box 752
Middle Island, New York 11953-0752

Dear Mr. Golstein:

It has come to our attention that you have somehow obtained and published in the 1991-1992 Winter edition of *2600 Magazine* portions of certain Bellcore proprietary internal documents.

This letter is to formally advise you that, if at any time in the future you (or your magazine) come into possession of, publish, or otherwise disclose any Bellcore information or documentation which either (i) you have any reason to believe is proprietary to Bellcore or has not been made publicly available by Bellcore or (ii) is marked "proprietary," "confidential," "restricted," or with any other legend denoting Bellcore's proprietary interest therein, Bellcore will vigorously pursue all legal remedies available to it including, but not limited to, injunctive relief and monetary damages, against you, your magazine, and its sources.

We trust that you fully understand Bellcore's position on this matter.

Sincerely,

LCSuchyta

[illegible]

Knowing Bellcore, they might just consider THIS proprietary. Such is life. Note the UNIX file path printed at the bottom of the letter. On some system somewhere, this letter exists... Our reply appears on the facing page. We'd like reader input on this.

Emmanuel Goldstein
Editor
2600 Magazine
PO Box 752
Middle Island, NY 11953
(516) 751-2600
(516) 751-2608 FAX

RETURN MAIL - CERTIFIED RECEIPT REQUESTED

July 20, 1992

Leonard Charles Suchyta
LCC 2E 311
290 W. Mt. Pleasant Avenue
Livingston, NJ 07039

Dear Mr. Suchyta:

We are sorry that the information published in the Winter 1991-92 issue of 2600 disturbs you. Since you do not specify which article you take exception to, we must assume that you're referring to our revelation of built-in privacy holes in the telephone infrastructure which appeared on Page 42. In that piece, we quoted from an internal Bellcore memo as well as Bell Operating Company documents. This is not the first time we have done this. It will not be the last.

We recognize that it must be troubling to you when a journal like ours publishes potentially embarrassing information of the sort described above. But as journalists, we have a certain obligation that cannot be cast aside every time a large and powerful entity gets annoyed. That obligation compels us to report the facts as we know them to our readers, who have a keen interest in this subject matter. If, as is often the case, documents, memoranda, and/or bits of information in other forms are leaked to us, we have every right to report on the contents therein. If you find fault with this logic, your argument lies not with us, but with the general concept of a free press.

And, as a lawyer specializing in intellectual property law, you know that you cannot in good faith claim that merely stamping "proprietary" or "secret" on a document establishes that document as a trade secret or as proprietary information. In the absence of a specific explanation to the contrary, we must assume that information about the publicly supported telephone system and infrastructure is of public importance, and that Bellcore will have difficulty establishing in court that any information in our magazine can benefit Bellcore's competitors, if indeed Bellcore has any competitors.

If in fact you choose to challenge our First Amendment rights to disseminate important information about the telephone infrastructure, we will be compelled to respond by seeking all legal remedies against you, which may include sanctions provided for in Federal and state statutes and rules of civil procedure. We will also be compelled to publicize your use of lawsuits and the threat of legal action to harass and intimidate.

Sincerely,

Emmanuel Goldstein

EG/ed

[illegible]

the view of a fed

by The Fed

Why don't they understand? Why do both sides think they understand?

I never dreamed when I began a journey to obtain my first "hacker magazine", specifically *Phrack*, that my days would end up much like they are today. Let me explain. I am a computer security specialist for a division of the United States federal government, which will go unnamed. I am not writing this article as a government representative, but as an individual. I had been a computer security analyst for a couple of years before obtaining my first modem. I spent most of my day massaging our mainframe security software to ensure our more than 8000 users could obtain and maintain their necessery access. I didn't have time to worry about hackers and really didn't understand much about what the press talked about anyway. Hackers seemed to be these super-intelligent, terrifying individuals I couldn't compete with in regards to technical knowledge and I wasn't about to try. It didn't seem to apply to our systems anyway.

After I started calling other computers and interacting with individuals, I decided to try to get a copy of *Phrack*, the magazine that super-hacker Knight Lightning published and was arrested for, mostly for publishing the 911 computer program (well at least that is what I thought at the time, based on things I had read and heard). It was frightening to even decide to pursue this venture. I had read that hackers could break into any computer system and that they were constantly breaking into credit reports and messing up people's lives. I wasn't anxious to become a target of the "underground." What I realize now is that most of the underground could care less about me and my ventures. I was simply flattering myself by believing that I was important enough to become a target...who gives a damn about me? The fed ego is something else, eh? It's out there though, thick as ever. I see it mostly when I try to introduce folks to "hacker material" such as *2600*. I once told a whole conference room full of security folks about 2600 and the benefits of receiving it. The responses from the audience were things like, "Yeah, but don't use your real name when you subscribe, these are hackers you know." One man even told me he was going to set up a fake name with a P.O. Box before ordering *2600*, to protect himself. I find it amazing that people think a magazine that supports itself from subscriptions is out to destroy its subscription base.

In my travels, I also wasn't sure if I should be honest about my position or assume a hidden identity. I mean, I could call a "hacker BBS" and say, "Hi, my name is ... and I am a fed. Can I have a copy of all your files? I just want to read them. Honest." I wasn't sure that I would get much success from that, but at the same time I was afraid if I did try to hide my real identity, those evil hackers would find out and destroy me. So, I signed on a bbs and said, "Hi, I'm a fed." You know what, it worked. I found out by being honest and to the point, folks were very helpful. The more I learned from interacting with the underground, the more I realized just how deceptive the government had been in a lot of regards (I don't trust mirrors in hotels anymore!). I was hoping by being honest, that others would realize that fed was not always equal to deception.

You know what else I found out? There are evil hackers, but they seem to be few and far between (of course these evil ones are the ones that have hacked my account!). Matter of fact, other hackers didn't even seem to accept them. Know what else I found out? The Secret Service really messed up on the Phrack case. Knight Lightning was patient enough to explain his side of the story to me and has filled me in on things the press "neglected to mention." Know what else? I realize now how clueless I was in regards to a lot of computer security issues. I know I am still clueless in a lot of regards and will always be, but I have learned so much over these past years that I now want to make an effort to educate others in the computer security arena of the benefits of knowing both sides of the story. Believe it or not, I am actually getting a chance to do that. I have been contacted by federal agencies that have learned of "my contacts in the underground" and wanted to use me as a buffer between them and the hacker community. One agency was interested in hiring some of "my trusted hacker friends" while another was interested in learning about hackers and "getting inside their heads." Additionally, non-government agencies have contacted me for much the same reasons. I'm not sure how the word of my interactions got around (well, I have a pretty good idea) but I actually think it funny in many ways. I see the same naive fear in these folks that I experienced myself when I started my journey to learn "the other side of the story." Now, I interact with as many if not more hackers during the day as I do security professionals and, as a result, my knowledge of the holes that exist in computer systems has increased immensely. I even learned enough to hack into one of our computer systems, expose our security holes, and get them fixed. As a security specialist, that is priceless to me. I was only able to do that because of the training I received from these so called notorious malicious hackers. Hackers helping to improve the security of government computer systems, hmmmmmm, seem suspect to you? Not to me. If I found a security weakness in a computer and wrote articles about it, published and sent it out so that thousands of folks could get it, I would expect the hole to be fixed. If I found that hole still open, I may become just a bit upset or assume it was an open invitation to violate the system. While underground files that explain these techniques have become a routine part of my day, there was a time I didn't even know they existed and certainly didn't know they existed to the extent they do. So part of the issue as to why they don't listen is that most of us have never heard the message.

I have accidentally tripped over holes in systems before and disseminated the information, only to be told that we could not put those controls in place because it would impact the operations of the organization, which it very well may do. It's a judgement call for management. Many security professionals are viewed as having tunnel vision (many of them do) and not understanding the operational end of the business. While many understand the holes that exist and have made every effort to get them fixed, management just won't let them.

One other thing I have learned by interacting with the computer underground is that sometimes us security folks aren't the only ones who are clueless. I have heard from hackers who said to me that they did not understand our side of many of the issues. One view that seems the most prevalent is that a security professional's real job is to keep people out of computer systems. That is a small part of what we do but the largest part of our job is ensuring that authorized users get the access they need to do their daily jobs. The main reason access is controlled on our systems is to ensure the integrity of the data we process. We want to ensure that our data is accurate. This is done by limiting the number of users that have certain access rights to it. Privacy is always an issue with sensitive data but we don't spend our days thinking "keep 'em out, keep 'em out." We are thinking "gotta give our users the access they need." Sometimes we just don't have the time to do anything else. That is why we don't always discover security holes in our systems. That is why many of them go unfixed. That is why picking up a magazine, like *Phrack* or *2600*, and learning the holes hackers are using to violate the systems we are trying to protect is so helpful. We may not have known that such holes existed without the underground's help. What is even better than reading it in an underground publication is having an email address of the author so that you can contact them and get further assistance. It has been an amazing tool for me.

I am going to continue to interact with the underground as long as I am able and will continue to lead other security professionals to that same interaction. I think only then does a person really begin understanding the true issues involved in security. I think only through this type of interaction does a person learn the rest of the story. It has made me realize more than anything else that both sides don't understand the factors affecting the others. Usually the main factor involved in preventing this is the ego and arrogance of the individuals on both sides, each of the players saying, "they just don't listen."

BOOK REVIEW

The Devouring Fungus (Tales of the Computer Age)
by Karla Jennings
Published in United States by:
W.W. Norton & Company, Ltd.
New York, NY
Published in Canada by:
Penguin Books Canada Ltd.
Newmarket, ONT
237 pages, $10.95 (United States), $14.95 (Canada)

Review by W. Ritchie Benedict

One of the new myths of the late 20th century is that women are supposed to loathe computers (although perhaps not as much as they are supposed to loathe professional football and hockey). Therefore, some may consider it unusual for a book to be written by a woman about computers, except -er- she appears to be poking fun at that oh-so-serious attitude programmers often have. It is well known there is such a thing as "urban legends" - these are stories someone swears once happened to a friend or a relative. What is not commonly known, until now that is, is that there is a veritable plethora of stories about the early days of computers. For example, the term "bug" for a software problem is supposed to have originated when a moth got caught in a relay on a Mark 1 back in 1945. Ms. Jennings says the term goes much further back - at least to Thomas Edison in 1878. It is a wonder that the whole field now seems so conventional, considering the eccentric geniuses who developed it. They range from absent minded Norbert Wiener, who walked around in a perpetual daze to Alan Turing (inventor of the famous test for determining whether a machine can think) - a tragic figure with severe sexual difficulties. Then there was John Von Neumann, who loved mathematical problems and games to such an extent that he once battled a five-year-old over who would be the first to play with some inter-locking building blocks.

The early days of cybernetics provide plenty of odd data. For example: Did you know that Helmut Hoelzer built a fully electronic analog computer in Nazi Germany in 1941? Babbage, the very first computer engineer, was a victim of his own endless drive for perfection? Only 45 years ago, in 1947, degrees in computer science did not exist?

Jennings really shines when she gets on to the subject of modern day computer hackers and the wildly humorous errors people make when they purchase equipment. She cites the elderly gentleman who very carefully folded a floppy disk in half before he left the store, the man who kept getting "Syntax Error" over and over after a clerk told him he should type in RUN to get the system functioning, and found after half an hour of confusion that the person was typing "ARE YOU IN?" Then there is the fellow who, after being instructed to "press any key to continue", complained he couldn't find the "ANY" key on the computer. Each chapter is prefaced with a computer gag. I know these things do happen - I once attempted to get a file decompressing program through my modem when I was first learning about such things. After a month of total frustration in attempting to get it to function, I dialed back and downloaded a second program. As soon as I got it up on the screen, I read the words: "The first program has a manufacturer's defect - do not use!"

Then there is the notorious computer virus - something I feel fortunate not to have encountered personally. In the early days (the almost prehistoric time of 1970!), they were relatively friendly, albeit annoying. Today, they have turned into something downright nasty. One recent virus caused $96 million in lost computer time and in the efforts to remove it. It is fortunate Gorbachev and glasnost came along when they did as one shudders at what might have happened if the computers for Reagan's Star Wars plan had malfunctioned. Jennings relates a number of instances where computer glitches have caused disastrous errors in expensive government projects. A single missing character destroyed the Mariner 1 Venus probe.

The devouring fungus of the title not only refers to an all consuming passion for computers, but also to an incident where a client of a major computer company was inexplicably losing data from magnetic tapes. After much investigation, it was discovered that old tapes had been stored in a room where a mycologist had been experimenting with fungi. This was in a large repository inside a mountain - a cavern designed to withstand nuclear attack. A fungus had attacked the tape, hitched a ride to data central and transmitted itself onto the read-write heads.

This book is a fast moving and amusing look at the world of the hacker and computer dweeb (a word containing a good deal of meaning according to the glossary that concludes the text). It is ideal for the computer buff and for the average reader who needs a laugh in what is an increasingly grim and dehumanized world.

2600 marketplace

2600 MEETINGS: New York City: First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., between Lexington and 3rd Avenues. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Washington DC:** In the Pentagon City mall from 5 to 8 pm on the first Friday of the month. **San Francisco:** At 4 Embarcadero Plaza (inside) from 5 to 8 pm on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6. **Los Angeles:** At the Union Station, corner of Macy St. and Alameda from 5 to 8 pm, first Friday of the month. Inside main entrance by bank of phones. Payphone numbers: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923, 9924; 213-614-9549, 9872, 9918, 9925. **Chicago:** Century Mall, 2828 Clark St., 5 pm to 8 pm, first Friday of the month, lower level, by the payphones. **St. Louis:** At the Galleria, Highway 40 and Brentwood, 5 pm to 8 pm, first Friday of the month, lower level, food court area, by the theatres. **Call 516-751-2600 to start a meeting in your city.**

LEARN HOW TO CREATE functional computer viruses with **THE LITTLE BLACK BOOK OF COMPUTER VIRUSES**. This book includes complete PC source code and detailed explanations of four new viruses. 190 pages. $14.95 postpaid or write for free details. American Eagle Publications, Box 41401, Tucson, AZ 85717.

PHONES TAPPED, office/home bugged, spouse cheating. Then this catalogue is for you! Specialized equipment, items, and sources. It's time to get even. Surveillance, countermeasures, espionage, personal protection. Send $5 check or money order to B.B.I., PO Box 579, Dept. 2-6, Shoreham, NY 11786.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

PRINT YOUR ZIP CODE IN BARCODE. A great label program that allows you to use a database of address to print label with barcode. You also type and print a custom label. Send $9 or check to: H. Kindel, 5662 Calle Real Suite 171, Goleta, CA 93117. IBM only.

GENUINE 6.5536 MHZ CRYSTALS only $5.00 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 104, Havertown, PA 19083. Also: information wanted on Northeast Electronics Corp's TTS-59A portable MF sender and TTS-37529 MF and loop signalling display. Need manuals, schematics, alignment and calibration instructions (or photocopies). Will reward finder.

WIRELESS MICROPHONE and wireless telephone transmitter kits. Featured in the WINTER 1991-92 2600. Complete kit of parts with PC board. $20 CASH ONLY, or $35 for both (no checks). **DEMON DIALER KIT** as reviewed in this issue of 2600. Designed and developed in Holland. Produces ALL voiceband signals used on worldwide telecommunications networks. Send $150 CASH ONLY (DM 350) to Hack-Tic Technologies, Postbus 22953, 1100 DL Amsterdam, Netherlands (allow up to 12 weeks for delivery). Please call +31 20 6001480 / *148. Absolutely no checks accepted!

FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Prolonks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

FOR SALE: Compaq Portable 386DX w/6MB RAM, 42MB HD, 1.2MB FD, 80387, tape backup, 2 expansion units, Ethernet board, VGA board, Hayes 2400B modem, Microsoft 400 DPI Mouse, DOS 5.0, manual, diskettes, tapes, etc. Virtually UNUSED - CPU still under warranty. $1,666 or best offer. (215) 358-5059.

TIN SHACK BBS (818) 992-3321. The BBS where hackers abound! Over a gig of files, many on-line games! Multi-line! 2600 Magazine readers get FREE elite access!

WOULD LIKE TO TRADE IDEAS with and befriend any fellow 2600 readers. Call Mike at 404-458 6561 if interested.

GET PAID FOR YOUR SKILLS: Basil Rouland is a small entrepreneurial firm providing information system security services to the government and private organizations. We are aggressively expanding our service capabilities and we are looking for talented people to join our team. We are currently recruiting individuals for our penetration testing and other services. Specifically we are looking for people with security experience in VMS, MPE, Primos, and Unix. Those with techniques in denial of service, spoofing, and other attacks via networks are also encouraged to promptly send us a resume and cover letter. The ideal candidate should be willing to travel, energetic, and creative. Possible security clearance for those seeking long term positions. Basil Rouland Inc., Suite 103, 5509 Roxbury Pl., Virginia Beach, VA 23463.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 9/15/92.

Voice Mail Hacking

by Night Ranger

I decided to write this article because I received numerous requests for voice mailboxes (VMB's) from people. VMB's are quite easy to hack, but if one doesn't know where to start it can be hard. To the best of my knowledge, this is the most complete text on hacking VMB systems.

VMB's have become a very popular way for hackers to get in touch with each other and share information. Probably the main reason for this is their simplicity and availability. Anyone can call a VMB regardless of their location or computer type. VMB's are easily accessible because most are toll-free numbers, unlike bulletin boards. Along with their advantages, they do have their disadvantages. Since they are easily accessible this means not only hackers and phreaks can get information from them, but feds and cares as well. Often they do not last longer than a week when used improperly. After reading this article and practicing the methods described, you should be able to hack voice mail systems with ease. With these thoughts in mind, let's get started.

Finding a VMB System

The first thing you need to do is find a virgin (unhacked) VMB system. If you hack on a system that already has hackers on it, your chance of finding a box is considerably less and it increases the chance that the system administrator will find the hacked boxes. To find a virgin system, you need to scan some 800 numbers until you find a VMB. A good idea is to take the number of a voice mail system you know, and scan the same exchange but not close to the number you have.

Finding Valid Boxes on the System

If you get a high quality recording (not an answering machine), then it is probably a VMB system. Try entering the number 100. The recording should stop. If it does not, you may have to enter a special key (such as '*' '#' '8' or '9') to enter the voice mail system. After entering 100 it should either connect you to something or do nothing. If it does nothing, keep entering 0's until it does something. Count the number of digits you entered and this will tell you how many digits the boxes on the system are. You should note that many systems can have more than one box length depending on the first number you enter. Example: Boxes starting with a six can be five digits while boxes starting with a seven can only be four. For this article we will assume you have found a four digit system, which is pretty common. It should do one of the following things:

1) Give you an error message, like "Mailbox xxxx is invalid."

2) Ring the extension and possibly connect you to a mailbox if there's no answer.

3) Connect you to mailbox xxxx.

If you don't get a valid mailbox then try some more numbers. Extensions usually have a VMB for when people are not at their extension. If you get an extension, move on. Where you find one box you will probably find more surrounding it. Sometimes a system will try to be sneaky and put one valid VMB per 10 numbers. Example: boxes would be at 105, 116, 121, etc. with none in between. Some systems start boxes at either 10 after a round number or 100 after, depending on whether it is a three or four box system. For example, if you do not find any around 100, try 110 and if you do not find any around 1000 try 1100. The only way to be sure is to try every possible box number. This takes time but can be worth it.

Once you find a valid box (even if you do not know the passcode), there is a simple trick to use when scanning for boxes outside of a VMB so that it does not disconnect you after three invalid attempts. What you do is try two box numbers and then the third time enter a box number you know is valid. Then abort (usually by pressing * or #) and it will start over again. From there you can keep repeating this until you find a box you can hack on.

Finding the Login Sequence

Different VMB systems have different login sequences (the way the VMB owner gets into his box). The most common way is to hit the pound (#) key from the main menu. This pound method works on most systems, including ASPEN's (more on specific systems later). It should respond with something like "Enter your mailbox." and then "Enter your passcode." Some systems have the asterisk (*) key perform this function. Another login method is hitting a special key during the greeting (opening message) of the VMB. On a CINDY or Q VOICE MAIL system you hit the zero (0) key during the greeting and since you've already entered your mailbox number it will respond with "Enter your passcode." If (0) doesn't do anything try # or *. These previous two methods of logging in are the most common, but it is possible some systems will not respond to these commands. If this should happen, keep playing around with it and try different keys. If for some reason you cannot find the login sequence, then save this system for later and move on.

Getting In

This is where the basic hacking skills become useful. When a system administrator creates a box for someone, they use what's called a default passcode. This same code is used for all of the new boxes on the system, and often on other systems too. Once the legitimate owner logs into his new VMB, they are usually prompted to change the passcode, but not everyone realizes that someone will be trying to get into their mailbox and quite a few people leave their box with the default passcode or no passcode at all. You should try all the defaults that are listed in the chart before giving up on a system. If none of the defaults work, try anything you think may be their passcode. Also remember that just because the system can have a four digit passcode the VMB owner does not have to have use all four digits. If you still cannot get into the box, either the box owner has a good passcode or the system uses a different default. In either case, move on to another box. If you seem to be having no luck, then come back to this system later. There are so many VMB systems that you should not spend too much time on one hard system.

If there's one thing I hate, it's an article that says "Hack into the system. Once you get in...." But unlike computer systems, VMB systems really are easy to get into. If you didn't get in, don't give up! Try another system and soon you will be in. I would say that 90 percent of all voice mail systems have a default listed above. All you have to do is find a box with one of the defaults.

Once You're In

The first thing you should do is listen to the messages in the box, if there are any. Take note of the dates the messages were left. If they are more than four weeks old, then it is pretty safe to assume the owner is not using his box. If there are any recent messages on it, you can assume he is currently using his box. Never take a box in use. It will be deleted soon, and will alert the system administrator that people are hacking the system. This is the main reason VMB systems either go down or tighten security. If you take a box that is not being used, it's probable no one will notice for quite a while.

Scanning Boxes From the Inside

From the main menu, see if there is an option to either send a message to another user or check receipt of a message. If there is you can search for virgin (unused) boxes without being disconnected like you would from outside of a box. Virgin boxes have a "generic" greeting and name: "Mailbox xxx" or "Please leave your message for mailbox xxx..." Write down any boxes you find with a generic greeting or name, because they will probably have the default passcode. Another sign of a virgin box is a name or greeting like "This mailbox is for ..." or a woman's voice saying a man's name and vice versa, which is the system administrator's voice. If the box does not have this feature, simply use the previous method of scanning boxes from the outside. For an example of interior scanning, when inside an ASPEN box, choose 3 from the main menu to check for receipt. It will respond with "Enter box number." It is a good idea to start at a location you know there are boxes present and scan consecutively, noting any boxes with a "generic" greeting. If you enter an invalid box it will alert you and allow you to enter another. You can enter invalid box numbers forever, instead of the usual three incorrect attempts from outside of a box.

Taking a Box

Now you need to find a box you can take over. Never take a box in use; it simply won't last. Deserted boxes (with messages from months ago) are the best and last the longest. Take these first. New boxes have a chance of lasting, but if the person for whom the box was created tries to login, you'll probably lose it. If you find a box with the system administrator's voice saying either the greeting or name (quite common), keeping it that way will prolong the box life, especially the name.

This is the most important step in taking over a box! Once you pick a box to take over, watch it for at least three days *before* changing anything! Once you think it's not in use, change only the passcode - nothing else! Then login frequently for two to three days to monitor the box and make sure no one is leaving messages in it. Once you are pretty sure it is deserted, change your greeting to something like "Sorry, I'm not in right now, please leave your name and number and I'll get back to you." *Do not* say "This is Night Ranger dudes..." because if someone hears that it's as good as gone. Keep your generic greeting for one week. After that week, if there are no messages from legitimate people, you can make your greeting say whatever you want. The whole process of getting a good VMB (that will last) takes about 7-10 days, the more time you take the better chance you have of keeping it for a long time. If you take it over as soon as you get in, it'll probably last you less than a week. If you follow these instructions, chances are it will last for months. When you take some boxes, do not take too many at one time. You may need some to scan from later. Plus listening to the messages of the legitimate users can supply you with needed information, such as the company's name, type of company, security measures, etc.

System Identification

After you have become familiar with various systems, you will recognize them by their characteristic female (or male) voice and will know what defaults are most common and what tricks you can use. The following is a list of a few popular VMB systems.

ASPEN (Automated SPeech Exchange Network) is one of the best VMB systems with the most features. Many of them will allow you to have two greetings (a regular and an extended absence greeting), guest accounts, urgent or regular messages, and numerous other features. ASPEN's are easy to recognize because the female voice is very annoying and often identifies herself as ASPEN. When you dial up an ASPEN system, sometimes you have to enter a * to get into the VMB system. Once you're in, you hit # to login. The system will respond with "Mailbox number please?" If you enter an invalid mailbox the first time it will say "Mailbox xxx is invalid...." and the second time it will say "You dialed xxx, there is no such number..." and after a third incorrect entry it will hang up. If you enter a valid box, it will say the box owner's name and "Please enter your passcode." The most common default for ASPEN's is either box number or box number plus 0. You only get three attempts to enter a correct box number and then three attempts to enter a correct passcode before it will disconnect you. From the main menu of an ASPEN box you can enter 3 to scan for other boxes so you won't be hung up like you would be from outside the box.

DEFAULTS	BOX NUMBER	TRY
box number (bn)	3234	3234 (Most Popular)
bn backwards	2351	1532 (Popular)
bn+0	323	3230 (Popular With ASPENs)

Some additional defaults in order of most to least common are:

4d	5d	6d
0000	00000	000000 (Most Popular)
9999	99999	999999 (Popular)
1111	11111	111111 (Popular)
1234	12345	123456 (Very popular with owners)
4321	54321	654321
6789	56789	456789
9876	98765	987654
2222	22222	222222
3333	33333	333333
4444	44444	444444
5555	55555	555555
6666	66666	666666
7777	77777	777777
8888	88888	888888

CINDY is another popular system. The system will start by saying "Good Morning/Afternoon/Evening. Please enter the mailbox number you wish..." and is easy to identify. After three invalid box entries the system will say "Good Day/Evening!" and hang up. To login, enter the box number and during the greeting press 0, then your passcode. The default for *all* CINDY systems is 0. From the main menu you can enter 6 to scan for other boxes so you won't be hung up on. CINDY voice mail systems also have a guest feature, like ASPEN's. You can make a guest account for someone, and give them a password, and leave them messages. To access their guest account, they just login as you would except they enter their guest passcode. CINDY systems also have a feature where you can have it call a particular number and deliver a recorded message. However, I have yet to get this feature to work on any CINDY boxes that I have.

MESSAGE CENTER is also very popular, especially with direct dials. To login on a MESSAGE CENTER, hit the * key during the greeting and the system will respond with "Hello <name>. Please enter your passcode." These VMB's are very tricky with their passcode methods. The first trick is when you enter an invalid passcode, it will stop you one digit *after* the maximum passcode length. Example: If you enter 1-2-3-4-5 and it gives you an error message after you enter the fifth digit, that means the system uses a four digit passcode, which is most common on MESSAGE CENTER's. The second trick is that if you enter an invalid code the first time, no matter what you enter as the second passcode it will give you an error message and ask again. Then, if you entered the correct passcode the second and third time it will let you login. Also, most MESSAGE CENTER's do not have a default. Instead, the new boxes are "open" and when you hit * it will let you in. After hitting * the first time to login to a box you can hit * again and it will say "Welcome to the MESSAGE CENTER" and from there you can dial other extensions. This last feature can be useful for scanning outside a box. To find a new box, just keep entering box numbers and hitting * to login. If it doesn't say something to the effect of welcome to your new mailbox then just hit * again and it will send you back to the main system so you can enter another box. This way you will not be disconnected. Once you find a box, you can enter 6 to record a message to send to another box. After hitting 6 it will ask for a mailbox number. You can keep entering mailbox numbers until you find a generic one. Then you can cancel your message and go back it out.

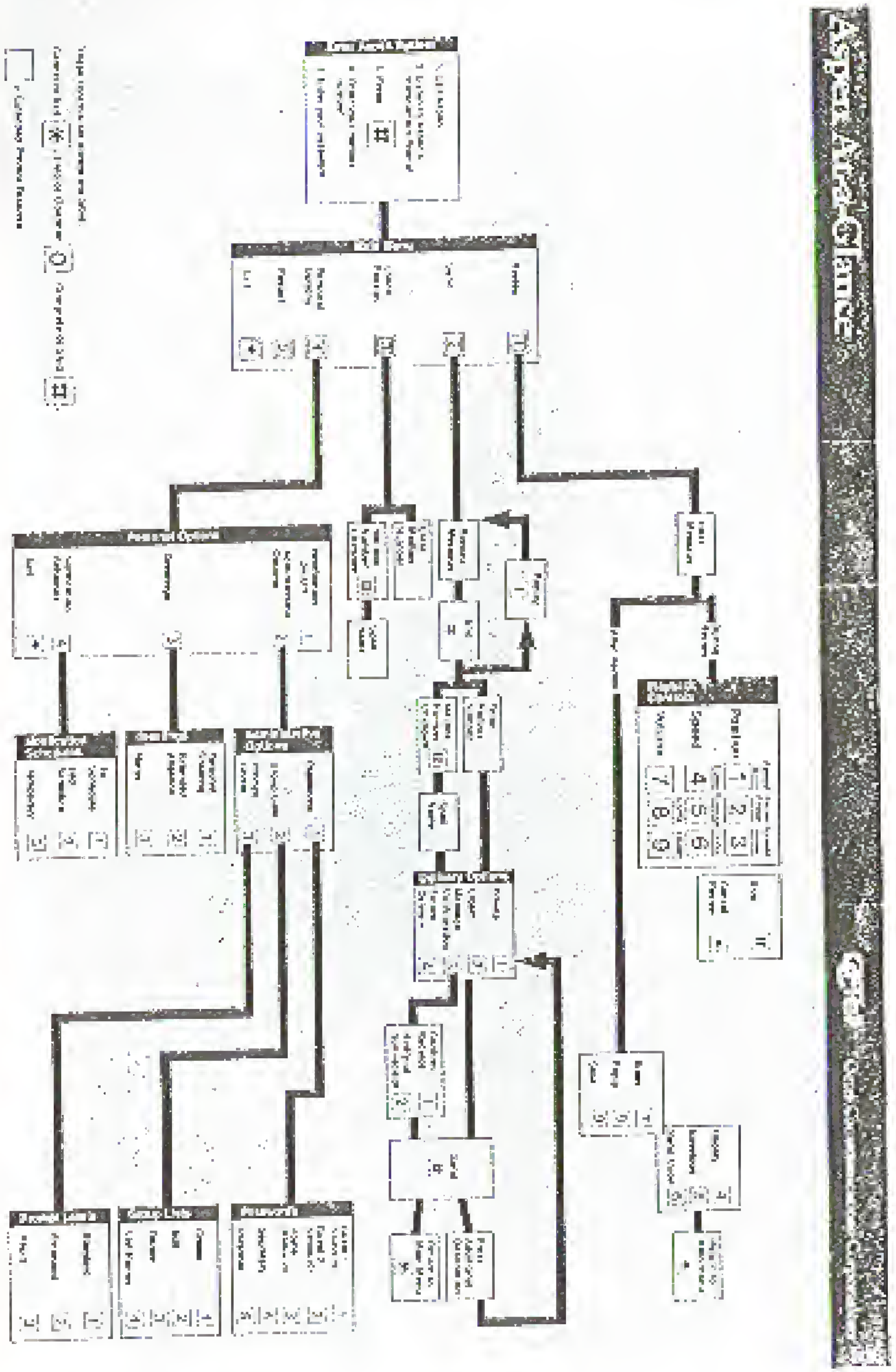
Q VOICE MAIL is a rather nice system but not as common. It identifies itself with "Welcome to Q VOICE MAIL Paging" so there is no question about what system it is. The box numbers are usually five digits and to login you enter 0 like a CINDY system. From the main menu you can enter 3 to scan other boxes.

There are many more systems I recognize but do not know the name for. You will become familiar with these systems too.

Conclusion

You can use someone else's VMB system to practice the methods outlined above, but if you want a box that will last you need to scan out a virgin system. If you did everything above and could not get a VMB, try again on another system. If you follow everything correctly, I guarantee you will have more VMB's than you know what to do with.

[illegible]		
[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
	[illegible]	
[illegible]	[illegible]	[illegible]



TIME TO RENEW?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

☎ ☎ ☎ ☎ ☎ ☎

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (the dire threats on this page will never apply to you)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25 □ 1989/$25 □ 1990/$25 □ 1991/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: □